Cisco Stealthwatch SaaS Test Drive Labs

Welcome to the Cisco Stealthwatch SaaS dCloud (Demo Cloud) Test Drive Labs! You will learn how to turn your network into a security sensor. Stealthwatch Cloud consists of two products, Private Network Monitoring (PNM) and Public Cloud Monitoring (PCM). This lab focuses on PNM use-cases, the lecture prior to the lab covers cloud monitoring topics. As part of this lab, you get hands on access to a pre-configured network with traffic that you generate to test live use cases including:

- Breach Detection
- Insider and Advanced Threat Detection
- High Risk Application Detection
- Policy Violations
- Encrypted Traffic Analytics

This lab lets you play the role of an attacker generating traffic; then you log into Stealthwatch Cloud as a defender to learn how to see and respond to these attacks. Completing these labs will help provide test plans to effectively use and operationalize Stealthwatch Cloud. Everything learned in these labs can be carried over into a production deployment of Stealthwatch.

Table of Contents

Requirements

1. Laptop with network capabilities
2. A Cisco.com account (go here to Register if you need one)
3. A Stealthwatch Cloud Portal (provided by lab proctor)

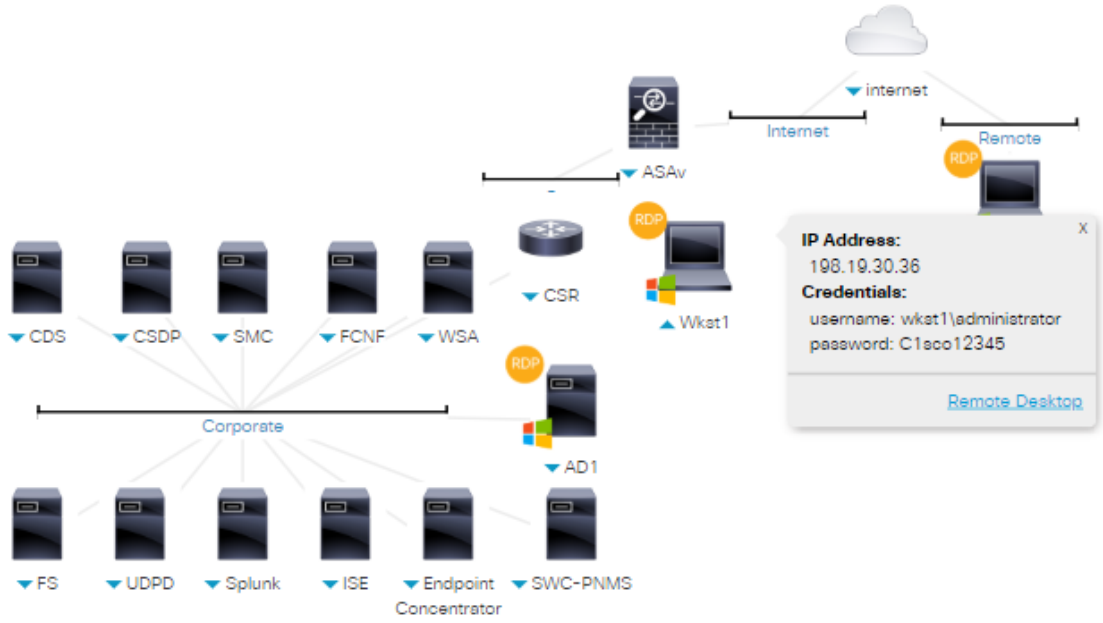
About This Test Drive Lab

The Cisco Stealthwatch Cloud Test Drive has been built as a training platform to gain first-hand experience using Stealthwatch Cloud SaaS. Students get to experience life-like cyber security attack situations in a virtualized enterprise lab environment, playing the role of an attacker and defender. Using an environment similar to many enterprise networks, students will learn and understand how their own environments get compromised, how security breaches get detected, and how to respond using Stealthwatch.

Topology & Accounts

This lab includes preconfigured users and components to illustrate scripted scenarios and features of Cisco Stealthwatch Cloud. Most components are fully configurable with predefined administrative user accounts. You can see the IP addresses and user account credentials to access a component by clicking on their icon in the Topology menu.

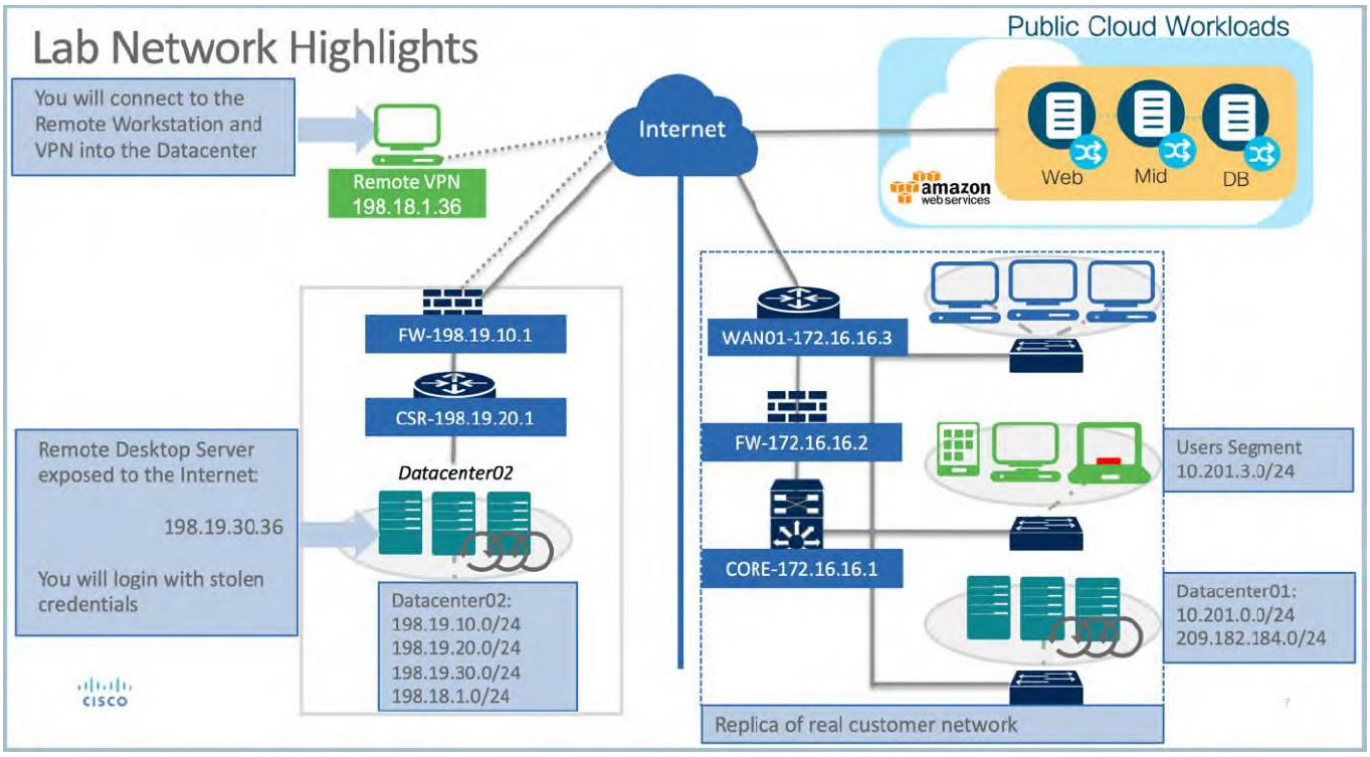
Figure 1. dCloud Topology



.

This lab includes preconfigured components such as ASA Firewalls, Cloud Services Routers, etc. Figure 2 highlights how the demo environment is setup. The majority of the exercises are done using Wkst1 via remote desktop.

Figure 2. Lab Setup



Accounts and Passwords for this dCloud Lab

Figure 3. Credentials

Username	Password	Endpoint Devices	IP Address
wkst1\Administrator	C1sco12345	Workstation1	198.19.30.36
admin	C1sco12345	Management Console	198.19.20.136
admin	C1sco12345	Flow Collector	198.19.20.137
admin	C1sco12345	Flow Sensor	198.19.20.138
admin	C1sco12345	UDP Director	198.19.20.139
admin	C1sco12345	Remote Workstation	198.18.1.36
admin	C1sco12345	Splunk	198.19.20.140
root	C1sco12345	CDS	198.19.20.134
admin	C1sco12345	CSR	198.19.10.2, 198.19.20.1, 198.19.30.1
admin	C1sco12345	ASAv	198.19.10.1, 198.18.133.100
dcloud\administrator	C1sco12345	AD1	198.19.20.10
admin	C1sco12345	WSA	198.19.20.51
admin	C1sco12345	ISE	198.19.20.141
admin	C1sco12345	Endpoint Concentrator	198.19.20.142
swcadmin	C1sco12345	SWC Sensor	198.19.20.143

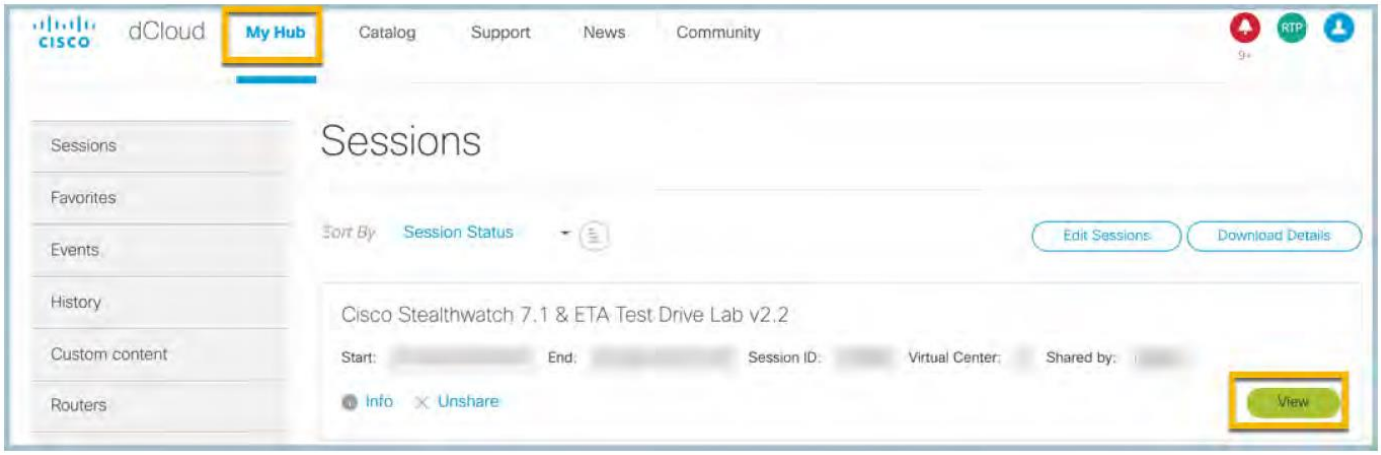
Getting Started

This lab allows you to familiarize yourself with dCloud. It walks through connecting to your shared session, validating the machine you will be connecting to in the data center and ensuring that Stealthwatch Cloud is up and available.

Let's begin.

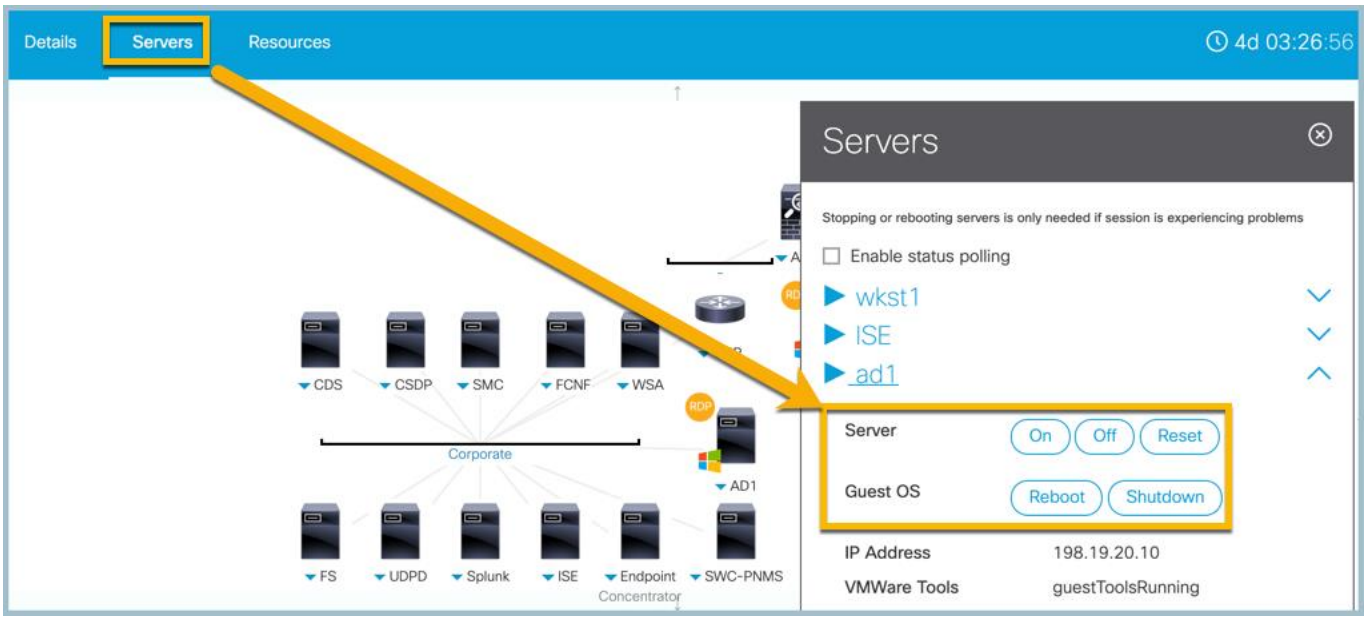
1. Login using your Cisco.com account to https://dcloud.cisco.com
2. Select My Hub, shown below. If you do not see an active session you may need to change to a different dCloud data center location. This is done by clicking the green circle in the upper right window. As your proctor which data center the lab is located in.
3. Select View for Cisco Stealthwatch 7.1 and ETA Test Drive Lab v2.2 session, shown below.

Figure 4. dCloud Session



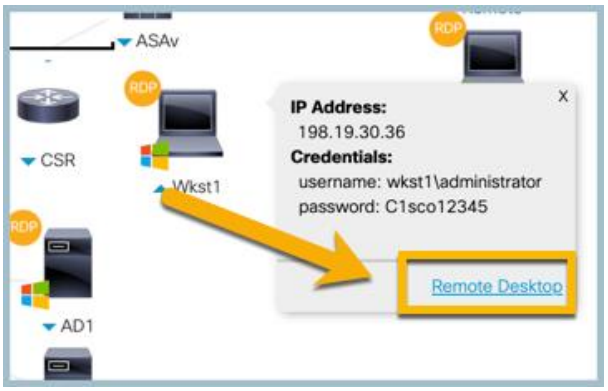
4. Select Servers to view the servers running for this lab.
5. The Servers tab pulls up all of the systems running with the lab environment. You have the ability to reboot the platforms from this location (e.g. reboot your windows workstation).

Figure 5. dCloud Services



6. To work within this lab, you will need to access Wkst1, which gives you access to all data center resources. Click Remote Desktop link to launch a web Remote Desktop session built within dCloud shown below.

Figure 6. Workstation1 Remote Desktop

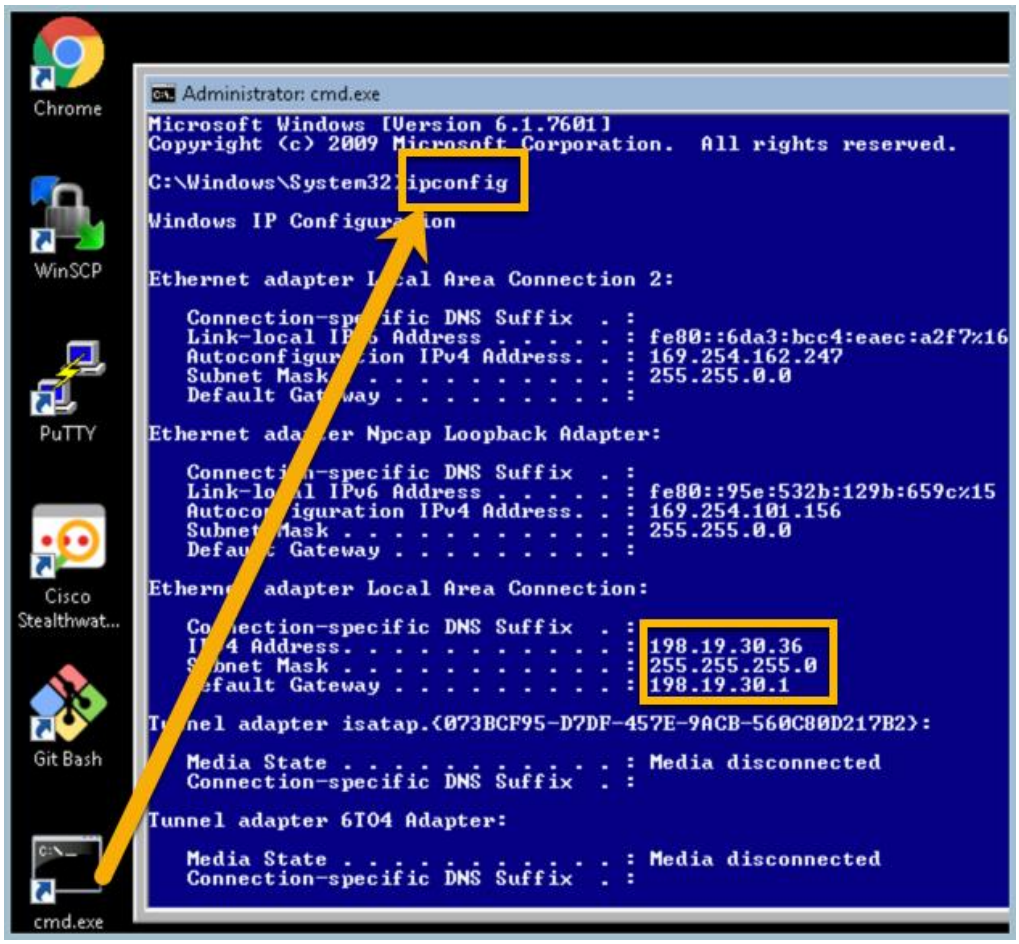


Validating Your Workstation 1 – ipconfig

Workstation 1 will be the Workstation you use. Let's validate the IP address of your Workstation 1. Refer to the figure below.

1. From the Workstation 1 click Start and type cmd in the search box.
2. Click cmd.exe from the search result.
3. Type ipconfig and hit enter.
4. Validate the IP address of your Workstation 1is 198.19.30.36. *Make note of this IP address because you will use it in most labs.*

Figure 7. Validate IP address of Workstation 1

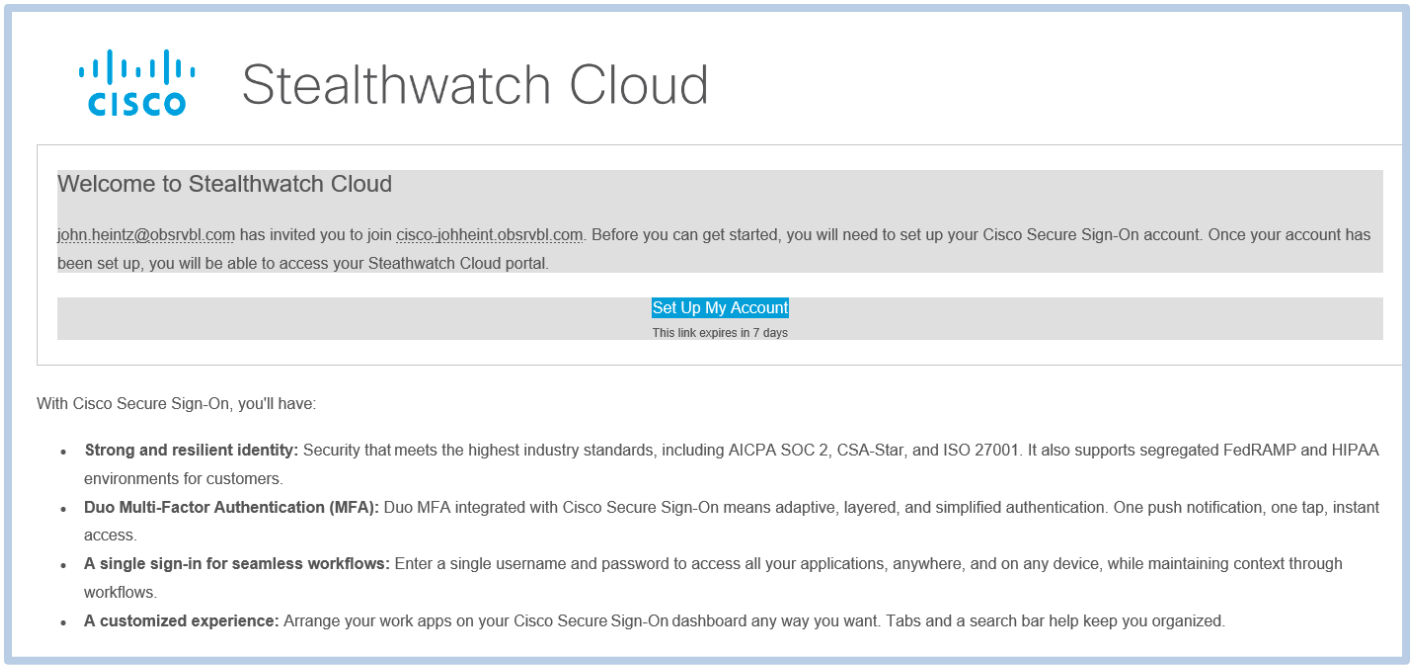


Access your Stealthwatch Cloud Account

As part of this Test Drive a new Stealthwatch Cloud portal was created. You will either have an invitation to the email attached to your CCO ID or the proctor will assign you a login at the beginning of the session.

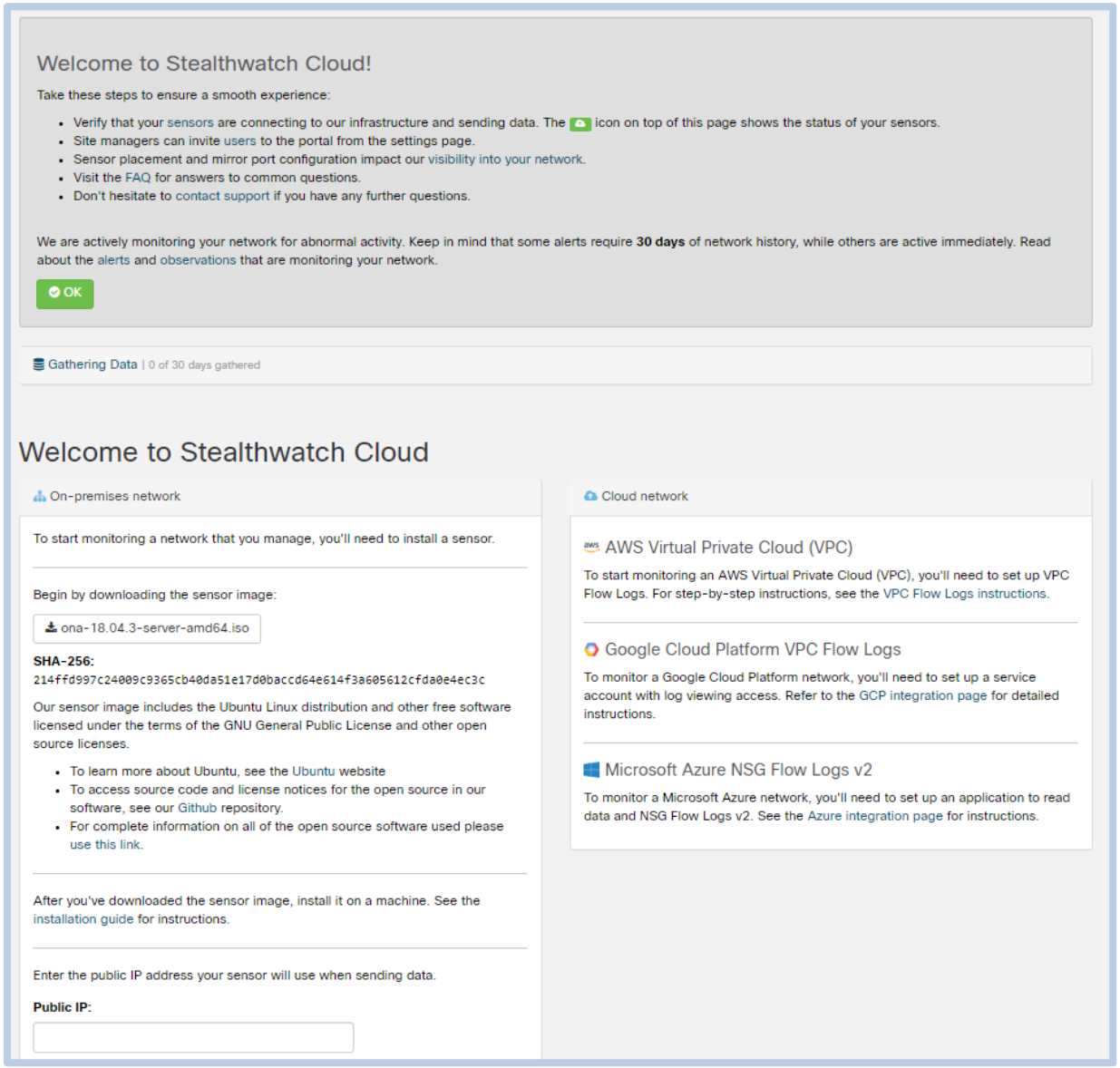
The email will be from service@obsrvbl.com. It will contain a onetime URL for creating your credentials. Additionally, since the portal is created unique to this Test Drive you will be attaching the Stealthwatch cloud virtual appliance (Flow Collector) in Dcloud to your cloud portal as well as some initial portal configurations.

Figure 8. Stealthwatch Cloud user registration



1. Register credentials using the link provided in the email
2. Login to the portal with the recently created credentials

Figure 9. New portal setup page



Initial setup of Stealthwatch Cloud

This lab uses a new Stealthwatch Cloud portal, as such we will be performing some initial steps to:

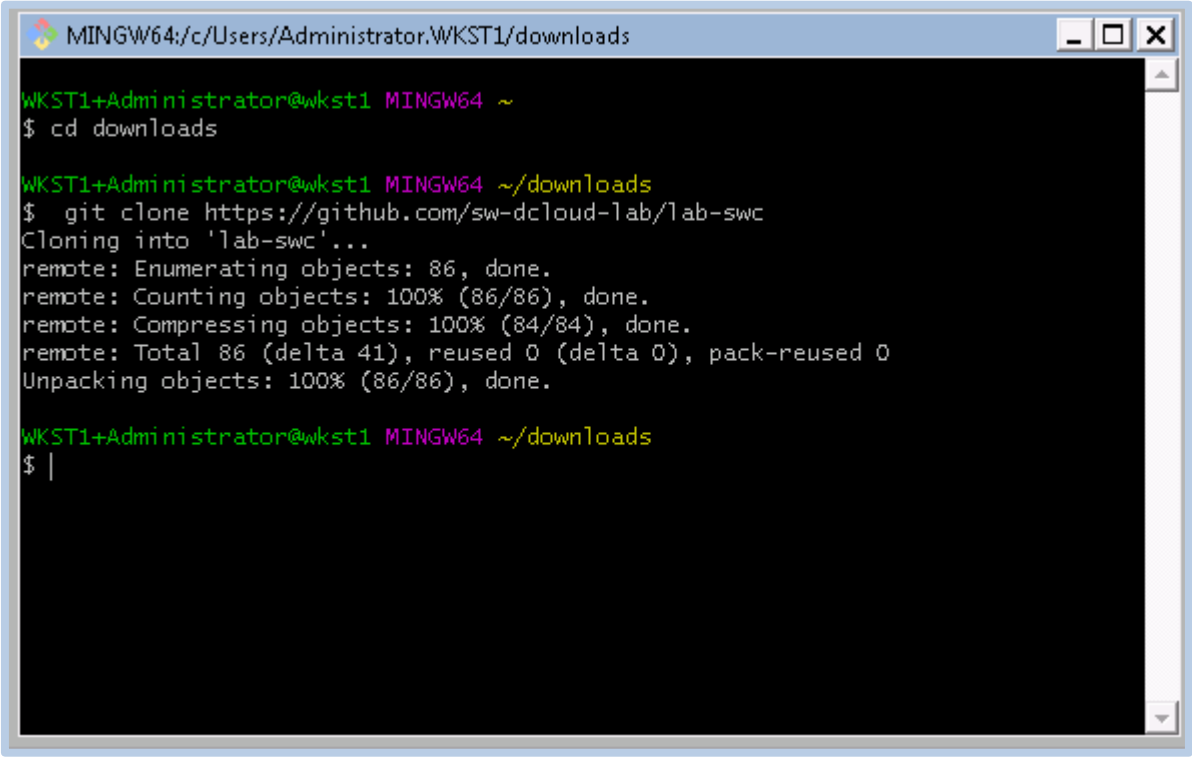
1. Use Gitbash to download scripts to the local machine for easier copy/paste operations
2. Forward NetFlow from the UDP Director to the Stealthwatch Cloud Sensor

3. Link the sensor the cloud portal and configure for enhanced NetFlow
4. Set some initial configurations in the portal.

Download scripts using GitBash

To make the lab easier we are hosting some of the scripts on GitHub, we will be using GitBash to download them to the local workstation.

Figure 10. GitBash

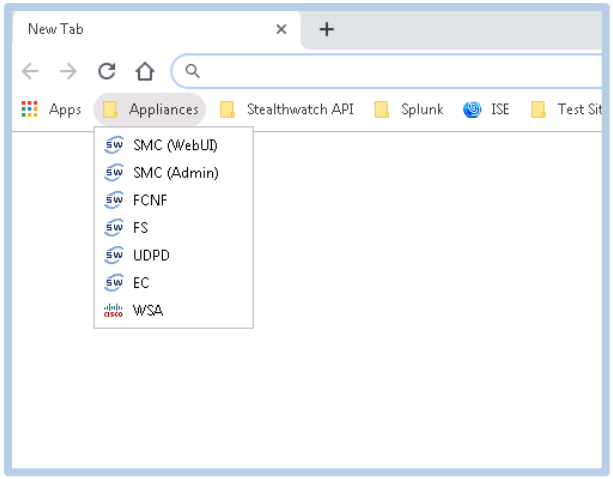


1. Open GitBash from desktop of Wkst1
2. Change directory to Downloads cd downloads
3. Type *git clone https://github.com/sw-dcloud-lab/lab-swc* to sync files to the workstation. This will copy files to the /downloads directory on the workstation and put them in the lab-swc folder.
4. Open downloads to confirm you have the lab-swc directory.

Configure UDP Director

1. Open the Chrome browser in Wkst1
2. Select SMC (WebUI) under Appliances, if you get a security warning click advanced then proceeed to 198.19.20.136. User is admin, password is C1sco12345

Figure 11. Location of SMC



3. We need to configure the UDP Director to forward flows to the Stealthwatch Cloud virtual appliance. Start by selecting UDP Director Configuration under the settings icon.
4. Next select Configure Forwarding Rules, this is listed under the Actions menu.

Figure 12. UDP Director Selection in SMC

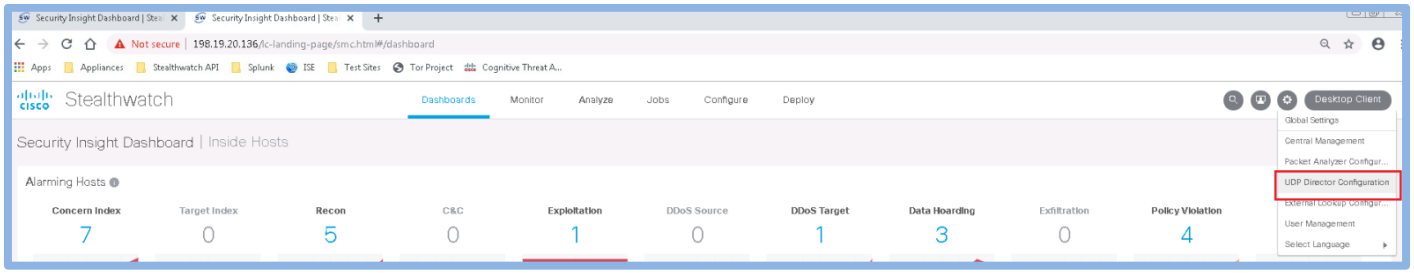
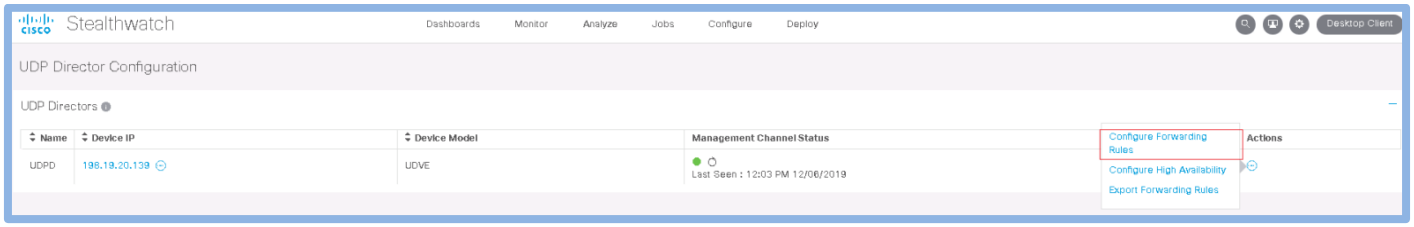


Figure 13. Configure Forwarding Rules



5. Select Import/Export, then Import Rules, select the XML file downloaded earlier using GitBash (downloads/lab-swc/UDPD-fwd-rules. xml. Note: Select Sync to save changes. The UDP Director is a Stealthwatch product for forwarding flows, in this lab we have multiple devices that need the flows, so we are using this to share the flows.

Figure 14. UDP Director Forwarding Rules

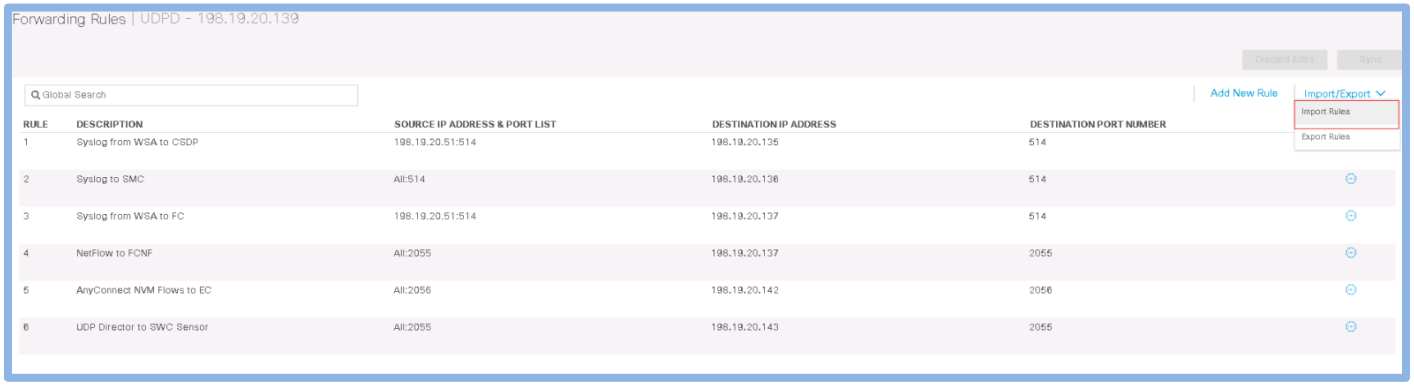


Figure 15. UDP Director Forwarding Rules after import

RULE	DESCRIPTION	SOURCE IP ADDRESS & PORT LIST	DESTINATION IP ADDRESS	DESTINATION PORT NUMBER	ACTION
1	Syslog from WSA to CSDP	198.19.20.51:514	198.19.20.135	514	
2	Syslog to SMC	All:514	198.19.20.136	514	
3	Syslog from WSA to FC	198.19.20.51:514	198.19.20.137	514	
4	NetFlow to FCNF	All:2055	198.19.20.137	2055	
5	AnyConnect NVM Flows to EC	All:2056	198.19.20.142	2056	
6	UDPD ASA to SWC Sensor	198.19.10.1:2055 172.16.16.2:2055	198.19.20.143	9997	
7	UDPD Netflow v9 to SWC Sensor	172.16.16.1:2055 172.16.16.3:2055 172.16.16.50:2055 172.16.16.100:2055 172.16.16.200:2055 198.18.128.138:2055 198.19.20.135:2055	198.19.20.143	9995	
8	UDPD ETA flow to SWC Sensor	198.19.20.1:2055	198.19.20.143	2055	
9	UDPD IPFIX to SWC Sensor	198.19.20.138:2055 198.19.20.142:2055	198.19.20.143	4739	

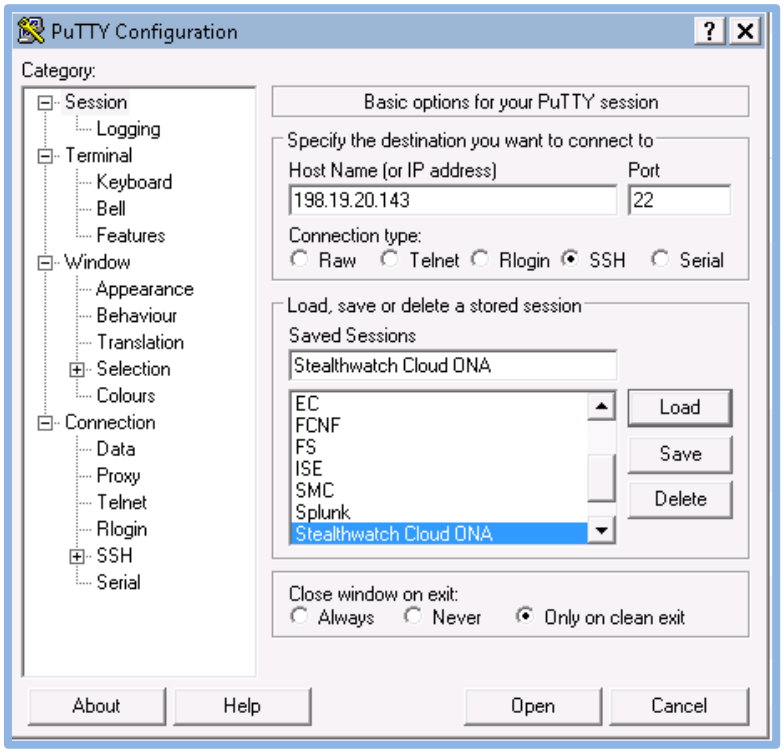
Configure Stealthwatch Cloud Sensor

In this next session we are going to setup the Stealthwatch Cloud sensor. Normally we would link a sensor to a cloud portal by finding the public IP address it is using to access the internet and entering it into the portal. However, dCloud shares public IP space we cannot use this method. This means more CLI fun for you as will be using the key for your portal to manually link the sensor.

Best Practice – Open your Stealthwatch Cloud portal inside the browser of Wkst1 so that you can copy/paste the key.

1. Next, we are going to configure some settings directly on the Stealthwatch Cloud virtual appliance. Open the swc_sensor_commands text file, this is a document we synced using GitBash earlier, it is located in /downloads/lab-swc. It contains the commands you can copy/paste that are referenced below.

Figure 16. Putty Window

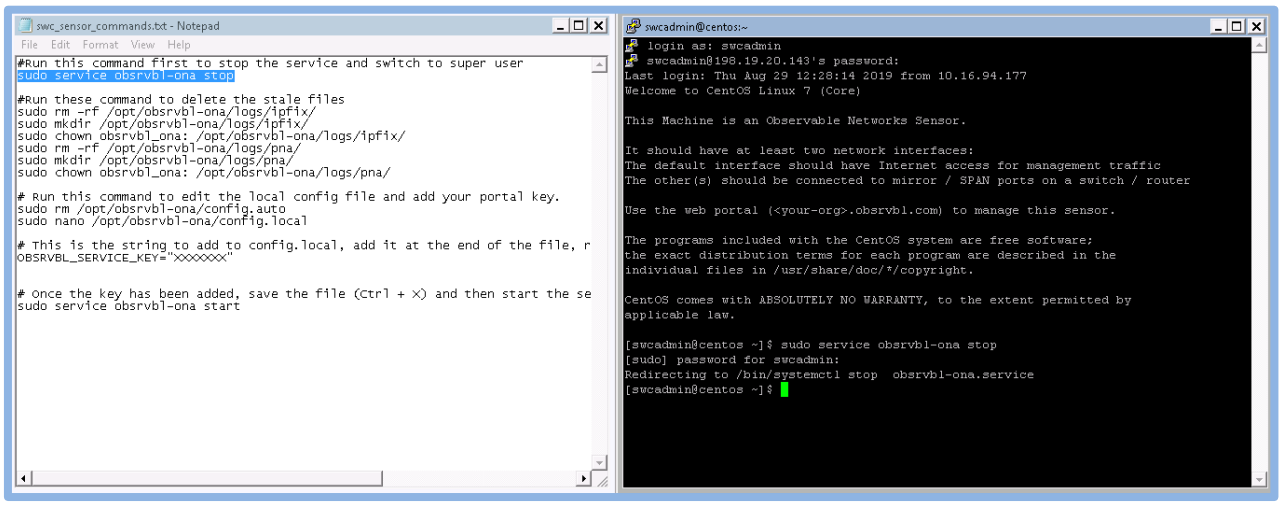


2. Open Putty on Wkst1
3. Select StealthWatch Cloud ONA

   Login as swcadmin, password is C1sco12345

4. Enter the first command after the # statement (, this will switch you to Super User and stop the Stealthwatch Cloud service. You will be prompted for your password again.

Figure 17. Stealthwatch Cloud CLI

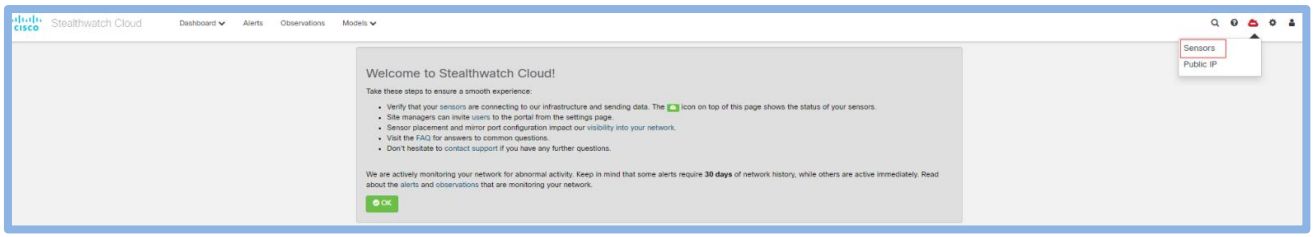


5. These next group of commands instructs the OS to remove any stale flow data files. Once a sensor is booted, the Stealthwatch Cloud service automatically starts collecting network data and queue's that data until it connects to a portal. In this case, we want to remove the old data and start fresh with our test drive. These commands are located in the "swc_sensor_commands.txt" document.

```
sudo rm -rf /opt/obsrvbl-ona/logs/ipfix/
sudo mkdir /opt/obsrvbl-ona/logs/ipfix/
sudo chown obsrvbl_ona: /opt/obsrvbl-ona/logs/ipfix/
sudo rm -rf /opt/obsrvbl-ona/logs/pna/
sudo mkdir /opt/obsrvbl-ona/logs/pna/
sudo chown obsrvbl_ona: /opt/obsrvbl-ona/logs/pna/
```

6. Next we be attaching the sensor to your portal. Since Dcloud re-uses the public IP space, we cannot use the normal method of using your public IP address. To work around this limitation, we will need to edit a config file on the sensor and manually add the key from your portal. The command for this is located in the "swc_sensor_commands.txt" file.
    a. Login to your Stealthwatch Cloud Portal
    b. In the upper left, select the cloud Icon
    c. Select Sensors

Figure 18. Service Key Location



    d. Scroll down to the bottom, copy the service key to the swc_sensor_commands.txt file. Use the line that starts with "OBSRVBL_SERVICE_KEY=
    e. Be sure to add quotes to the beginning and end of the key string. When finished it should look like figure 19.

f. Run the series of commands in the swc_sensor_commands.txt file that are for editing the local config file and adding the portal key. This will edit a file called confg.local. You will paste the service key into this file (location doesn't matter). After finished it should look like figure 20.

g. Hold Control + O to save, hit enter at save location prompt

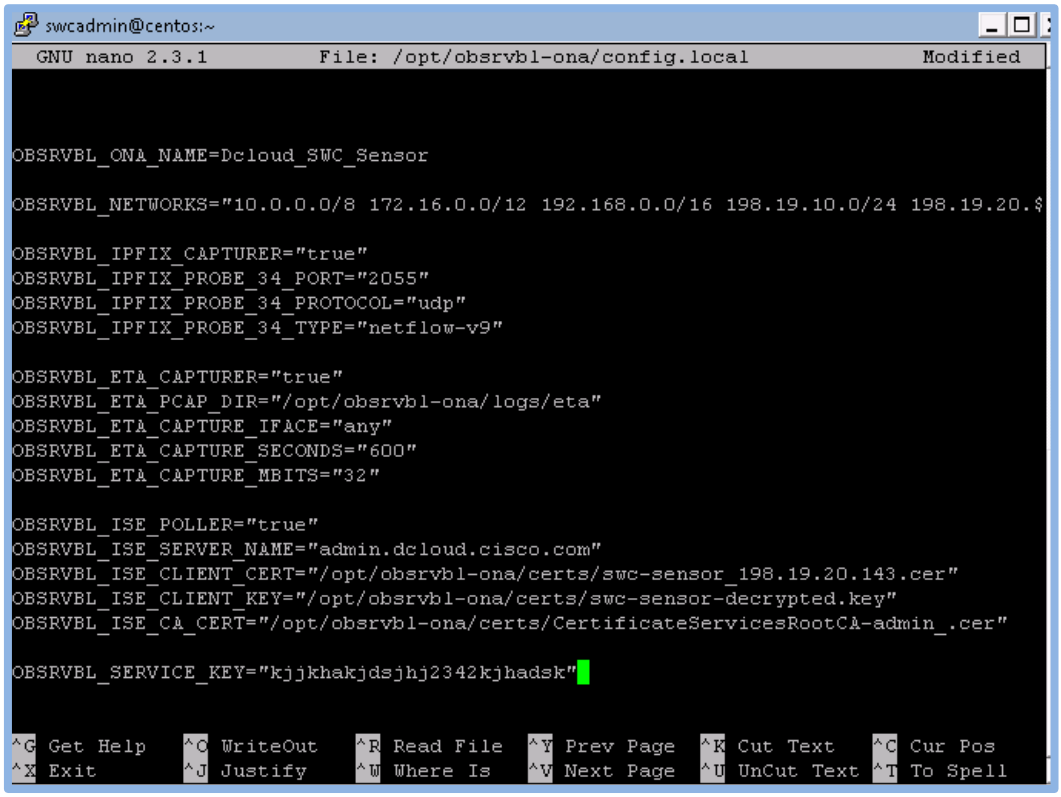
h. Hold Control + X to exit

i. Run the last command in the swc_sensor_commands.txt to restart the Stealthwatch service

Figure 19. Service Key in the text file

```
# This is the string to add to config.local, add it at the end of the file, replace xxx with they key from your portal.
OBSRVBL_SERVICE_KEY="kjjkhakjdsjhj2342kjhadsk"
```

Figure 20. Service key in the config.local file.



Once the key has been added and the service started on the sensor, it will begin a heartbeat process to announce and start a sync with the cloud portal. This process *usually* takes about 15 minutes to fully complete. When finished the sensor icon will be green and the name of the sensor will appear in the sensor list. We will continue working in the lab while this happens in the background.

Initial Stealthwatch Cloud Portal Configuration

Configure public subnet used in Dcloud in your SWC portal.

Since this is a new portal, we need to tell it what subnets are being used in Dcloud.

1. Login to the Stealthwatch Cloud portal
2. Select the settings icon on the upper right corner then Subnets, see figure 21.
3. Select Upload CSV, use the subnet.csv file that was downloaded using GitBash. (downloads/lab-swc/subnets.csv)

Figure 21. Subnet location

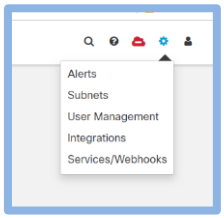
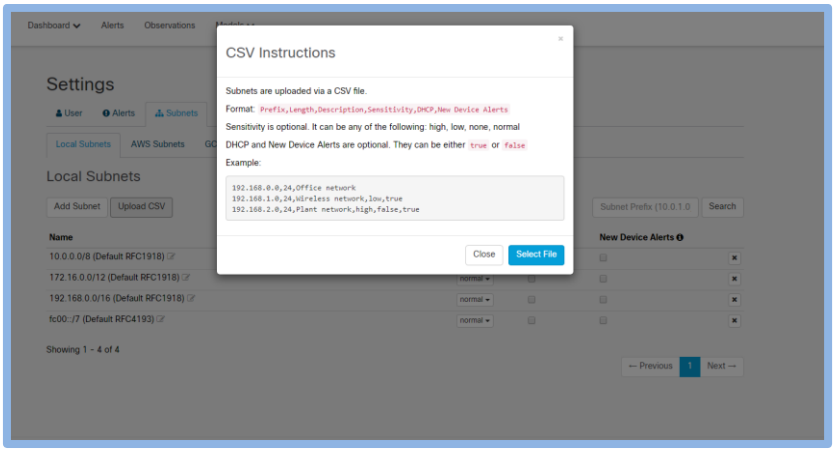
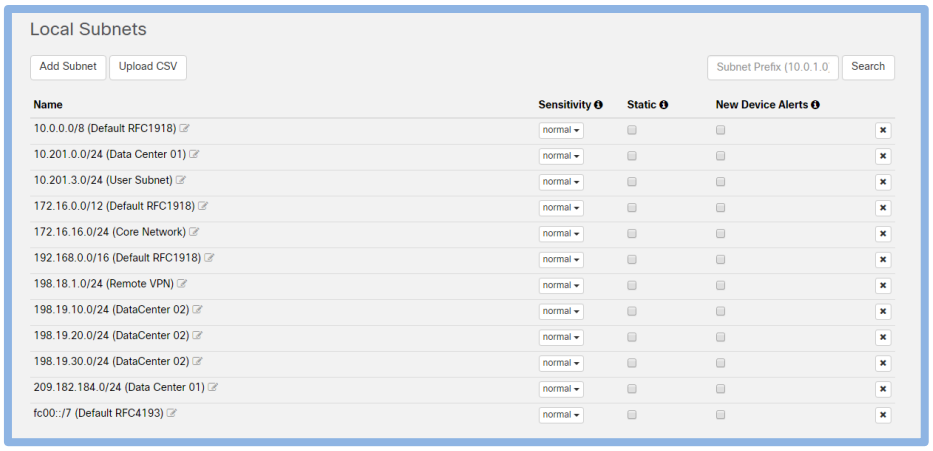


Figure 22. Subnet CSV Upload



4. Once uploaded the subnet labels will match what is configured in Dcloud

Figure 23. Local Subnets

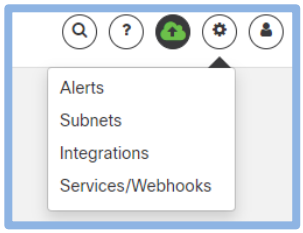


Configure a TOR Watchlist in the Stealthwatch Cloud portal

In this company using the TOR network is prohibited. We are going to configure the Stealthwatch Cloud portal to pull TOR exit nodes from a 3rd party website allowing us to see if users are using that service. The watchlist URL is located in the wkst1_command.text file for easy copy/paste into the portal

1. Login into the Stealthwatch Cloud portal
2. Select Alerts in the upper right-hand window

Figure 24. Alerts Menu

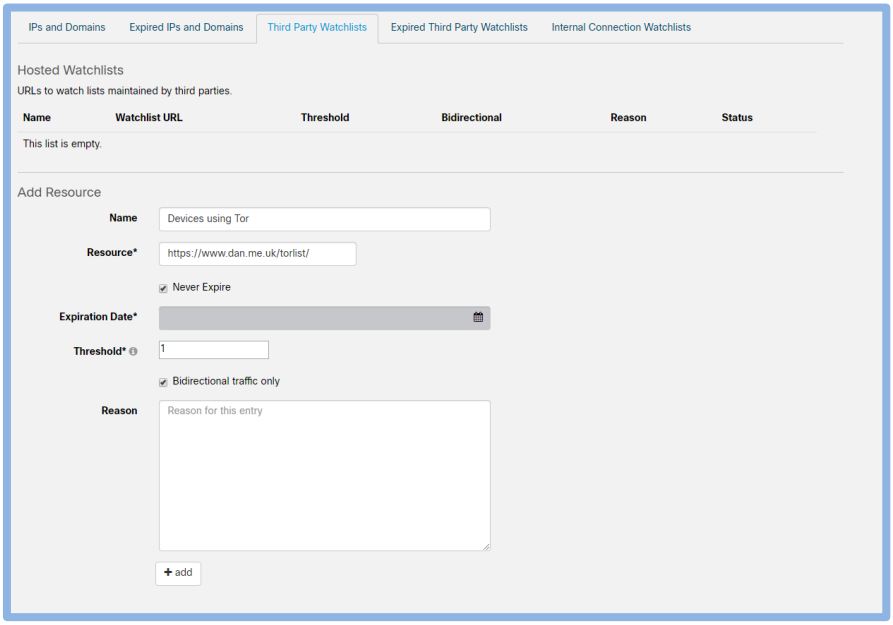


3. Select Configure Watchlists
4. Select Third Party Watchlists
5. Enter a description in the name field.

Note – The link below is located in the wkst1_commands.txt file located in /downloads/lab-swc

a. Resource = https://onstatic.s3.amazonaws.com/oneoff/combined_tor.txt
b. Check Never Expire
c. Check Bidirectional Traffic
d. Select Add

Figure 25. Third Party Watchlist

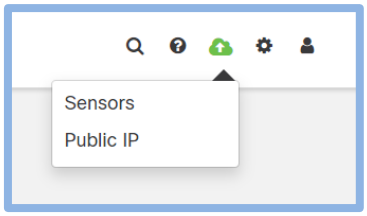


Sensor NetFlow Collection

The sensor you added previously should now be available in the portal. You will need to configure the flow settings that we imported to the UDP Director.

1. Select cloud icon in the upper left, then sensors.

Figure 26. Sensors Icon



2. Select the Change Settings button on the Dcloud sensor, then select the NetFlow/IPFIX tab, configure the settings as show in figure 28.

Figure 27. Active Sensors

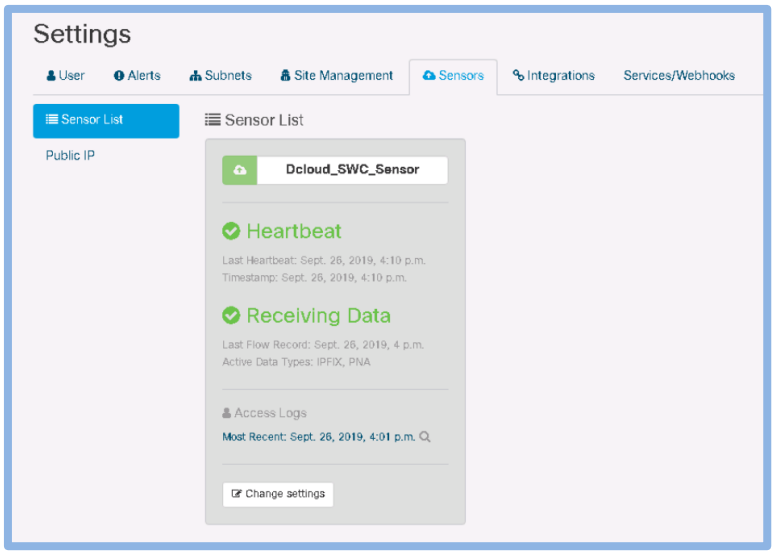
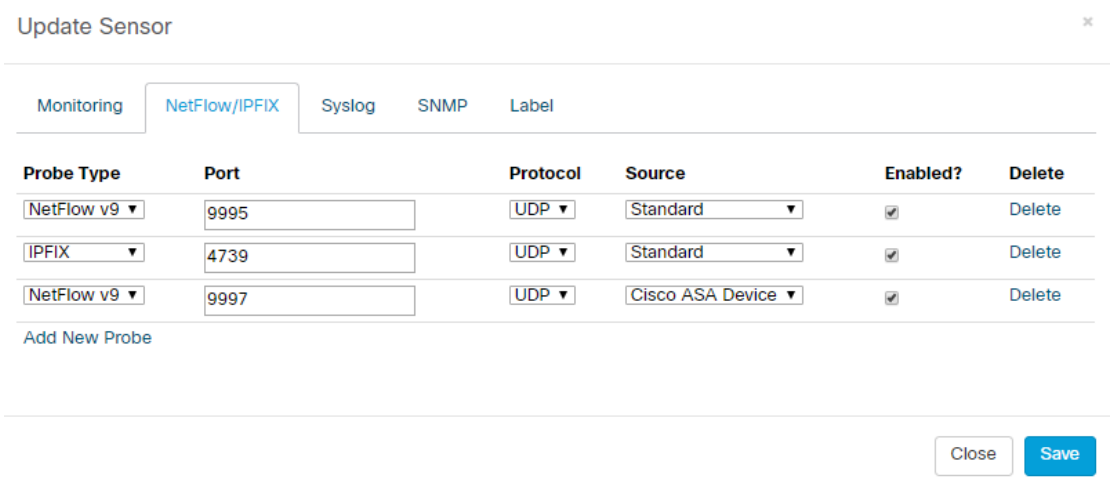
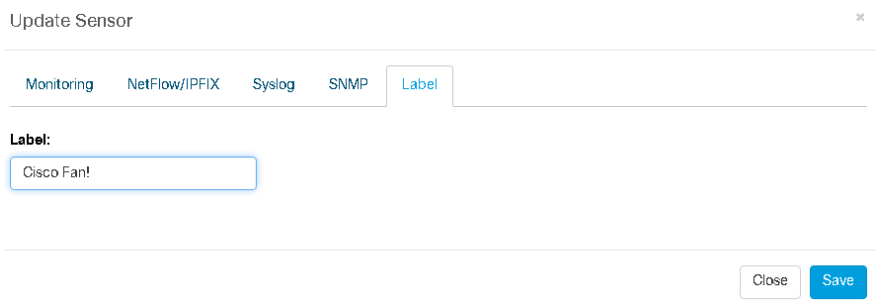


Figure 28. Flow Configuration Settings



3. Next set the sensor label to a personalized name, do this by selecting Label and entering a name. Select Save to save both changes. The sensor periodically checks the portal for updates, when a new configuration is detected it updates /opt/obsrvbl-ona/config.auto.



At this point the sensor is collecting data and sending to the Stealthwatch Cloud back-office ~every 15 minutes. You can see the last time a heartbeat and data were collected by clicking on the Green cloud icon.

The active data types show what the sensor is collecting, the default configuration of the sensor is to create flow data from any traffic on any of its network interfaces. This is mainly used for networks that are feeding the sensor with SPAN. However, it will also generate flows for the traffic hitting the management interface even if SPAN is not used, flows created from interface traffic show up as “PNA”. If a sensor is configured and able to receive flow traffic such as IPFIX or NetFlow then the “IPFIX” data type will also be displayed. In this lab

we would expect to see both. Initially it will display PNA, once the NetFlow configuration is pushed down and files are uploaded IPFIX will be displayed.

Figure 29. Sensor Status

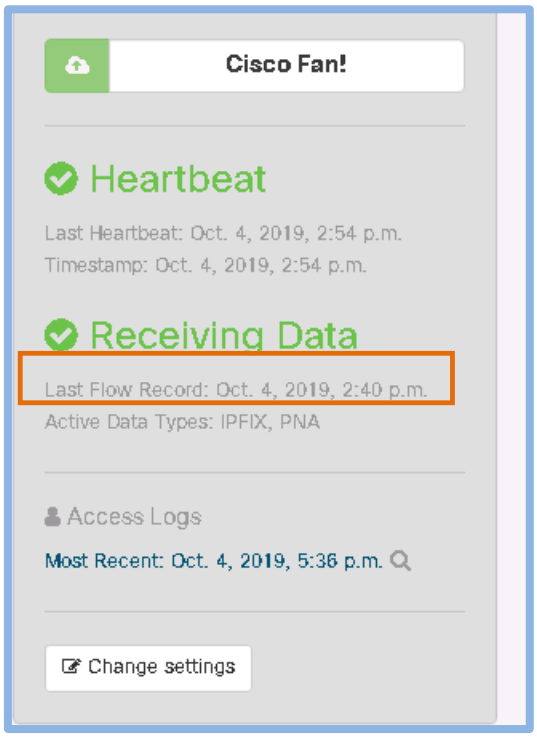
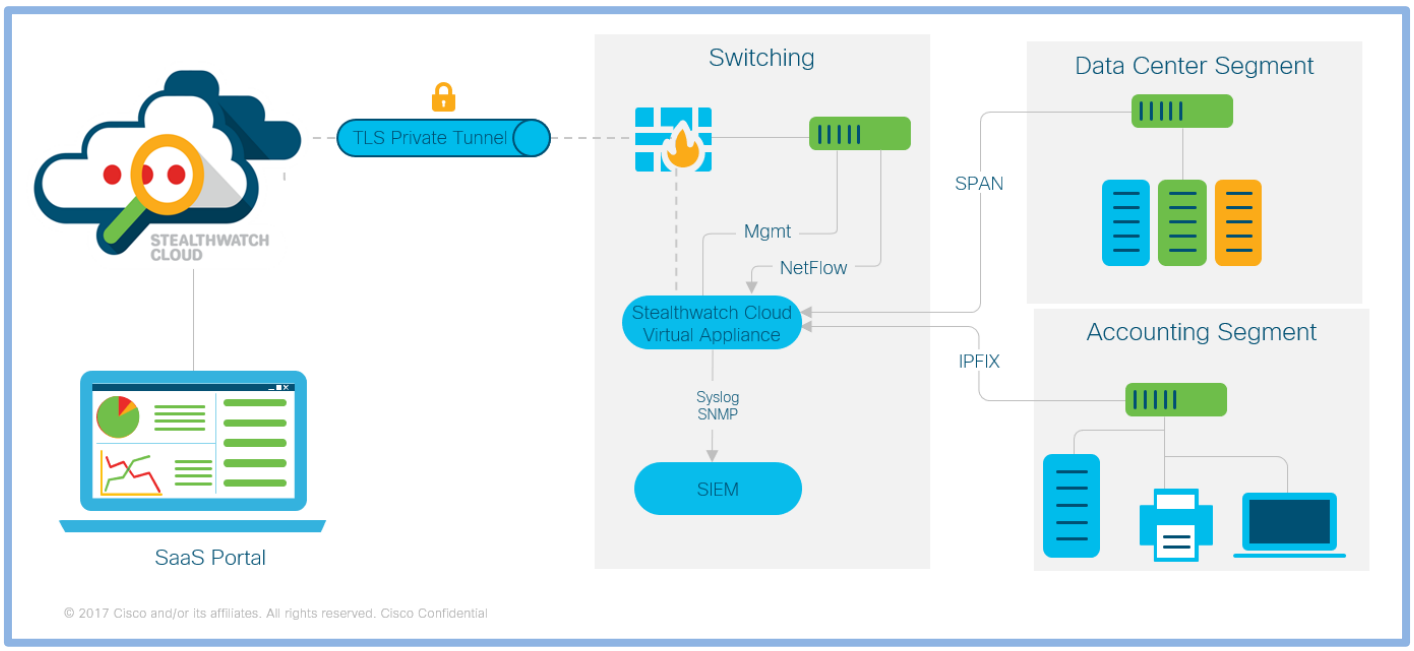


Figure 30. Sensor Network Deployment Capabilities and Options



Workstation Setup and Portal Overview

Validating Your Workstation 1 – Install Tor Browser

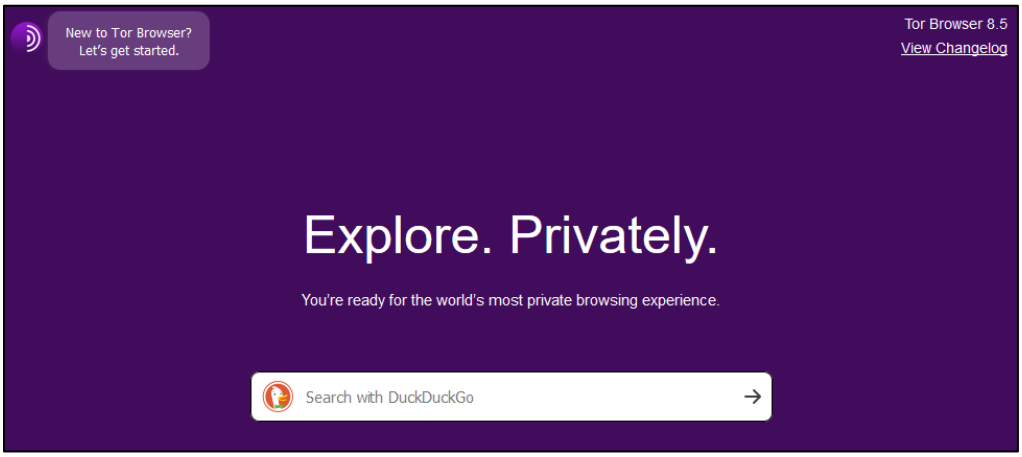
In this lab, you will install the Tor browser to generate traffic and validate results. All network traffic generated by the Workstation 1will be accounted for by NetFlow records, stored as a network audit trail and used to detect threats east and west inside the network and north and south to the Internet. Refer to screenshot shown below.

1. Open Chrome from the desktop of the Workstation 1 and select the Tor Project Link in the browser or go to https://www.torproject.org/download
2. Click the Windows Sig to Download Tor install file.
3. Install torbrowser .exe using all default settings. Make note of the file size of the .exe download which is ~52 MB; you will search for this in an upcoming lab.

Figure 31. Install Tor Browser

4. Click Start Tor Browser from the desktop, click Connect when Tor launches and search for "what is flexible NetFlow", shown below.
    a. Skim through a few articles and perform other searches to generate traffic through the Tor network. Make note that everything being searched is encrypted through the browser.
    b. Keep Tor Browser open for the next exercise.

Figure 32. Search within the Tor Browser



Validating Your Workstation 1 – netstat

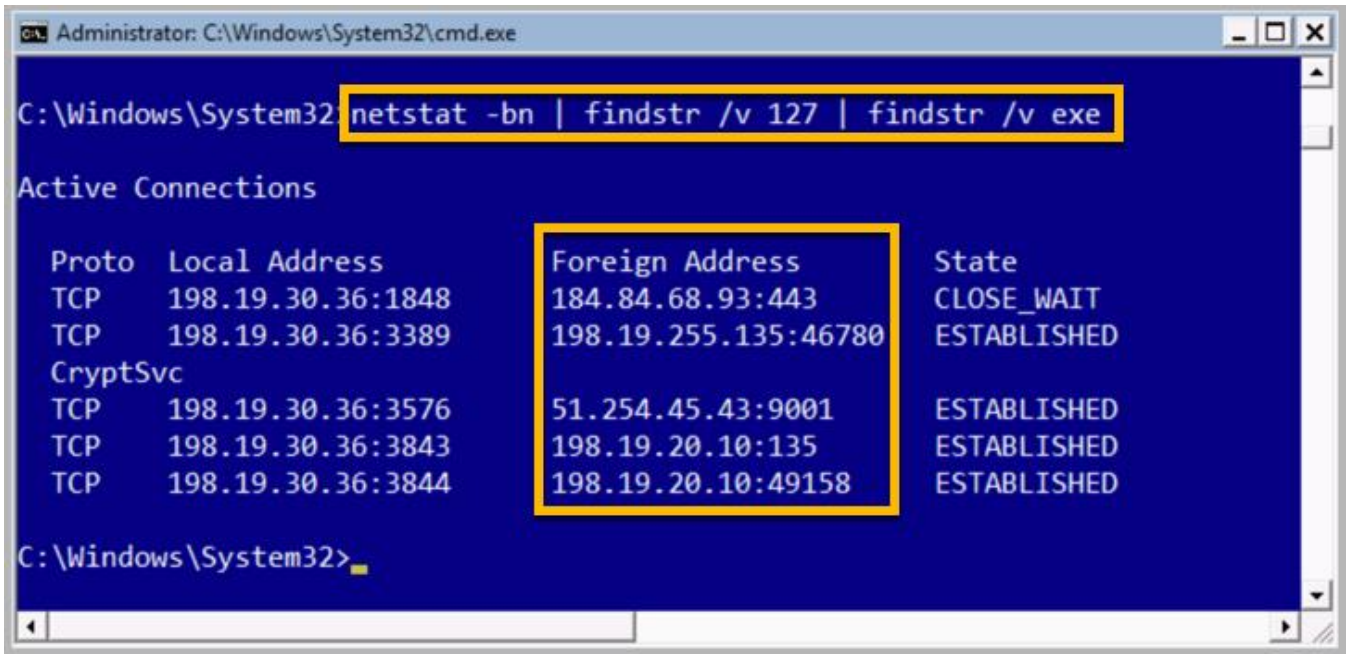
This lab will use the netstat (network statistics) command line tool to display incoming and outgoing network connections from Wkst1. It will also show that those connections will be accounted for through NetFlow. You are using netstat to see what connections exist to validate being able to search Stealthwatch for any active or historical network conversations.

The Wkst1 commands are also located in the Wkst1_commands.txt file in the downloads/lab-swc directory for easier typing. From the cmd.exe window, type netstat -bn | findstr /v 127 | findstr /v exe

The '-n' is needed to not perform name resolution so you can see the Foreign IP address being connected to. The '-b' will display process name. The findstr /v command will filter the results to display less information as shown below. Make note of the Foreign IP addresses being connected to. You will be able to search Stealthwatch for historical network conversations to and from the WKST1 IP address.

Note: Leave the command prompt open for later use

Figure 33. netstat utility

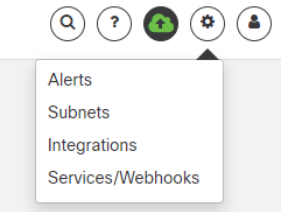


Configure Country Watchlists in the Stealthwatch Cloud portal

Stealthwatch Cloud Geo-codes all the IPs to their origin country. Stealthwatch Cloud allows users to configure which country represent "high-risk" for their organization. Traffic to a high-risk country is flagged with special observations, in addition if certain actions are seen from one of those countries, such as a remote login, an alert would be generated. In this lab we are going to select the United States, Germany, France, China, and any other you would like. Later in a future exercise we will review how to see the results of doing this.

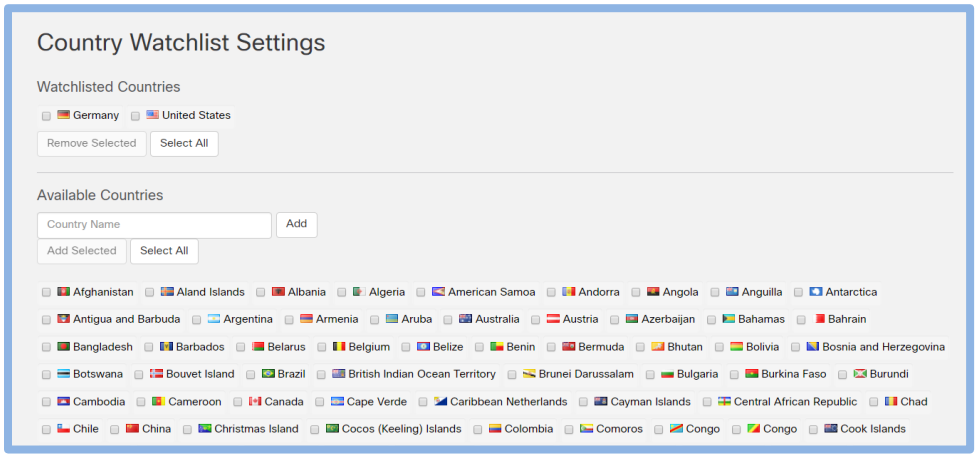
1. Login into the Stealthwatch Cloud portal
2. Select Alerts in the upper right-hand window

Figure 34. Alerts Menu



3. Select Configure Country Watchlists
4. Select the United States, Germany, France, China, and any other you would like, then select Add Selected

Figure 35. Country Watchlist Settings



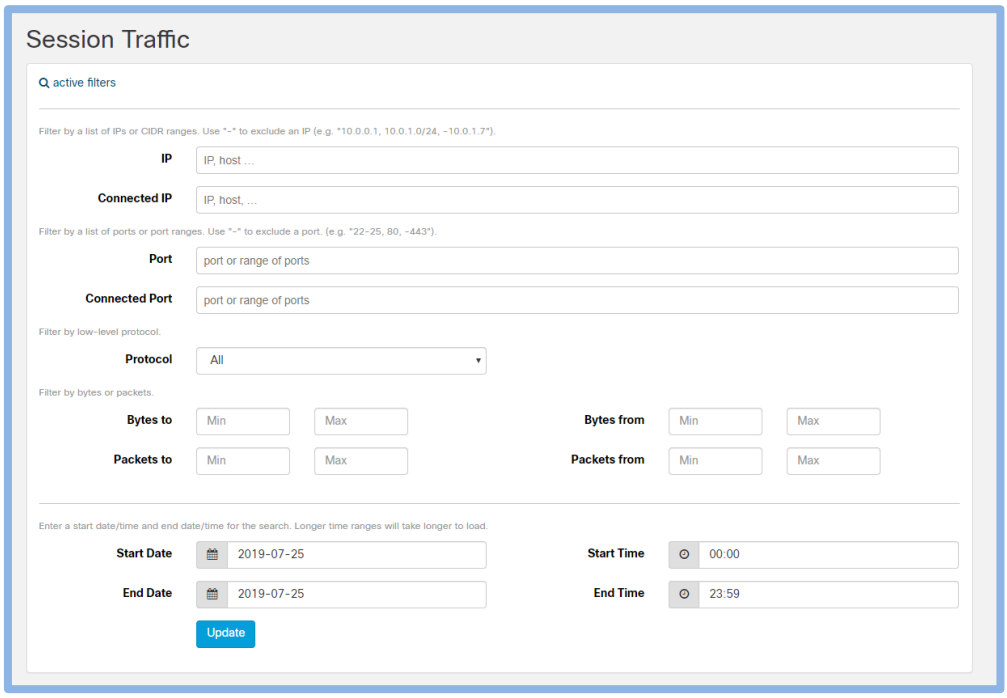
Stealthwatch Cloud – Flow Search

The Workstation 1 IP address has been validated and the connections established. You will query Stealthwatch Cloud to become comfortable with how NetFlow is collected and you can query against it. A later lab will provide a deeper understanding of NetFlow.

1. Login to your Stealthwatch Cloud portal, via Wkst1.

2. Select Models > Session Traffic from the menu bar. Session Traffic is used to query against the database of flows that Stealthwatch Cloud has. For example, you could run a query to see what DNS servers are being used, who is hosting web servers, etc.

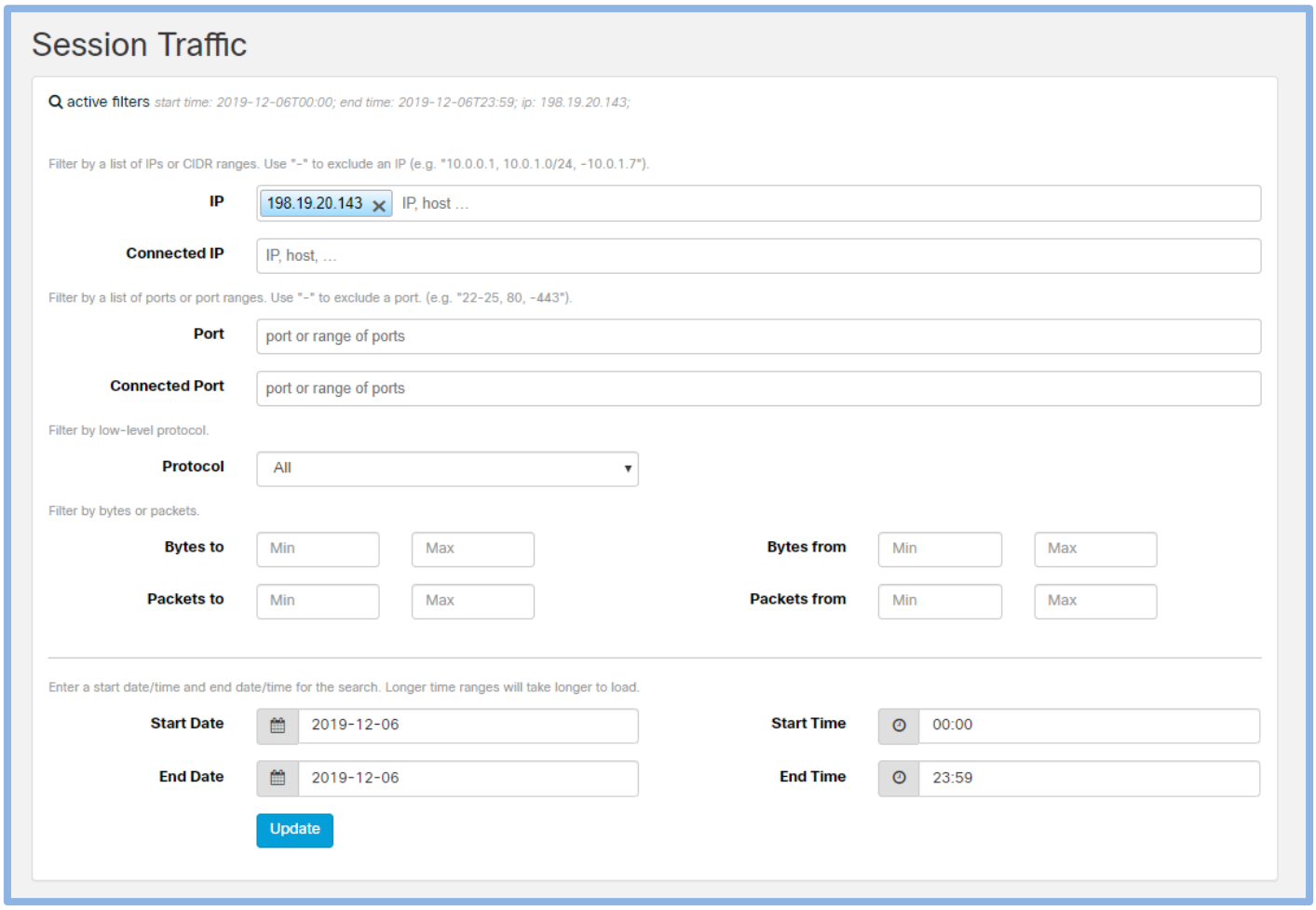
Figure 36. Stealthwatch Cloud Flow Query



The top portion of the Flow Search window will show the filter criteria. In this sample query we are going to look at the communication the sensor has been making.

1. Enter the Stealthwatch Cloud Sensor address of 198.19.20.143 into the IP field.
2. Enter 443 in the Connected Port. Note: that we are limiting the flow query to encrypted https or 443/tcp connections.
3. Leave Connected IP empty, this will allow to search for any 443 sessions.
4. Hit Update to begin running the flow query of any connection on this day between your sensor and the Internet on 443/tcp, as shown below.

Figure 37. Filter settings



1. Click the black triangle next to an external IP address to see more context about it or perform additional searches. Select Talos Intelligence to see more details on what Talos knows about the external IP address.

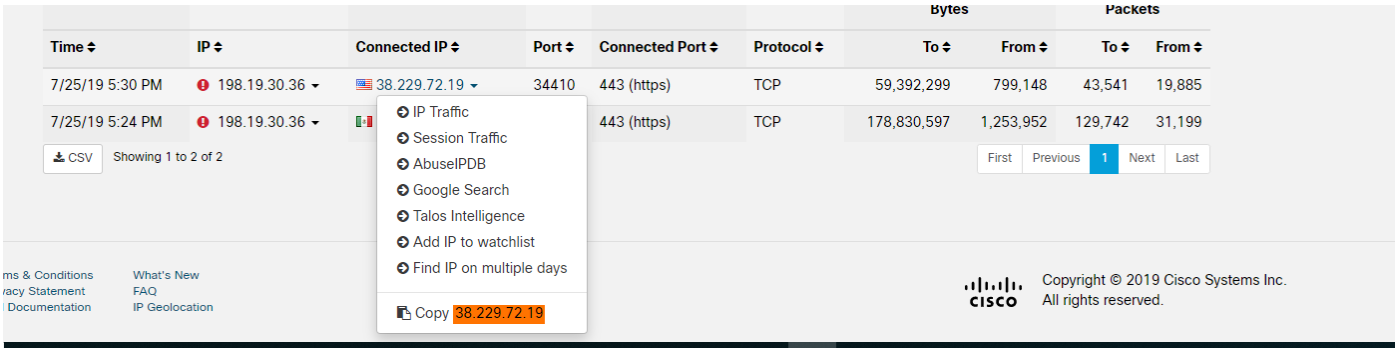
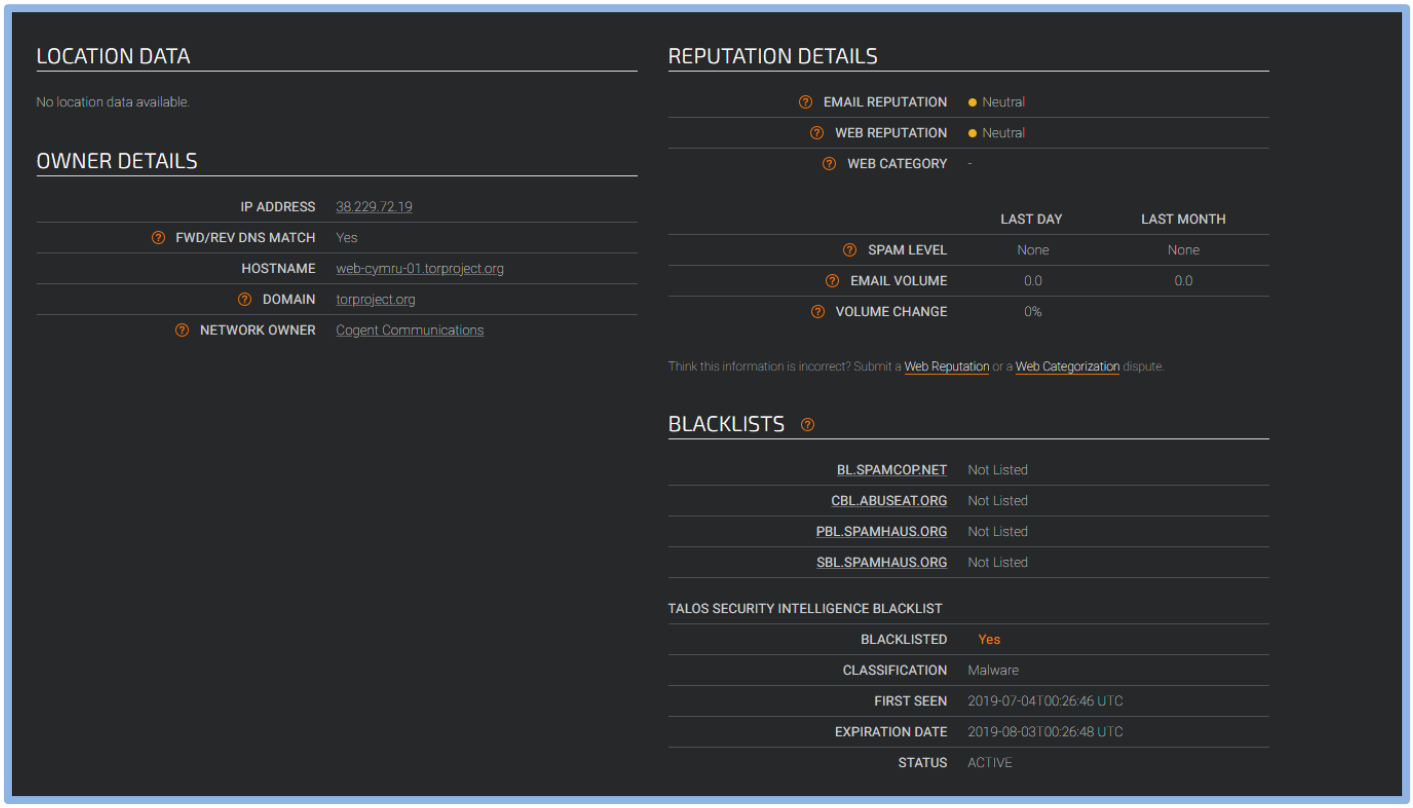


Figure 38. Talos Threat Intel Pivot



2. Add an external IP address to a watchlist by clicking the down arrow and selecting add to watchlist list, name the watchlist whatever you would like.

Figure 39. Custom watchlist pivot

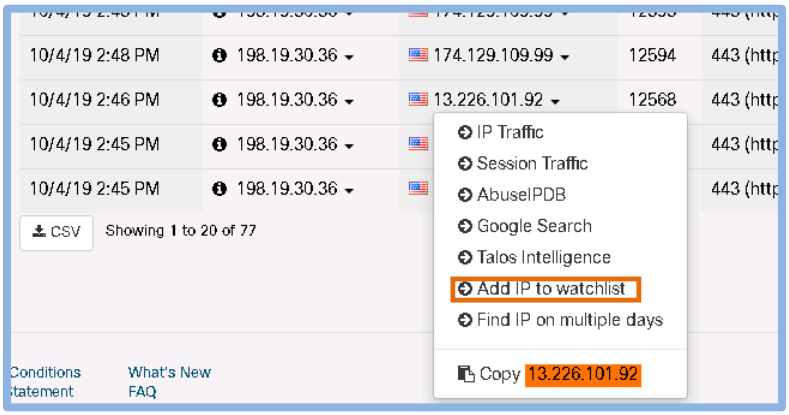
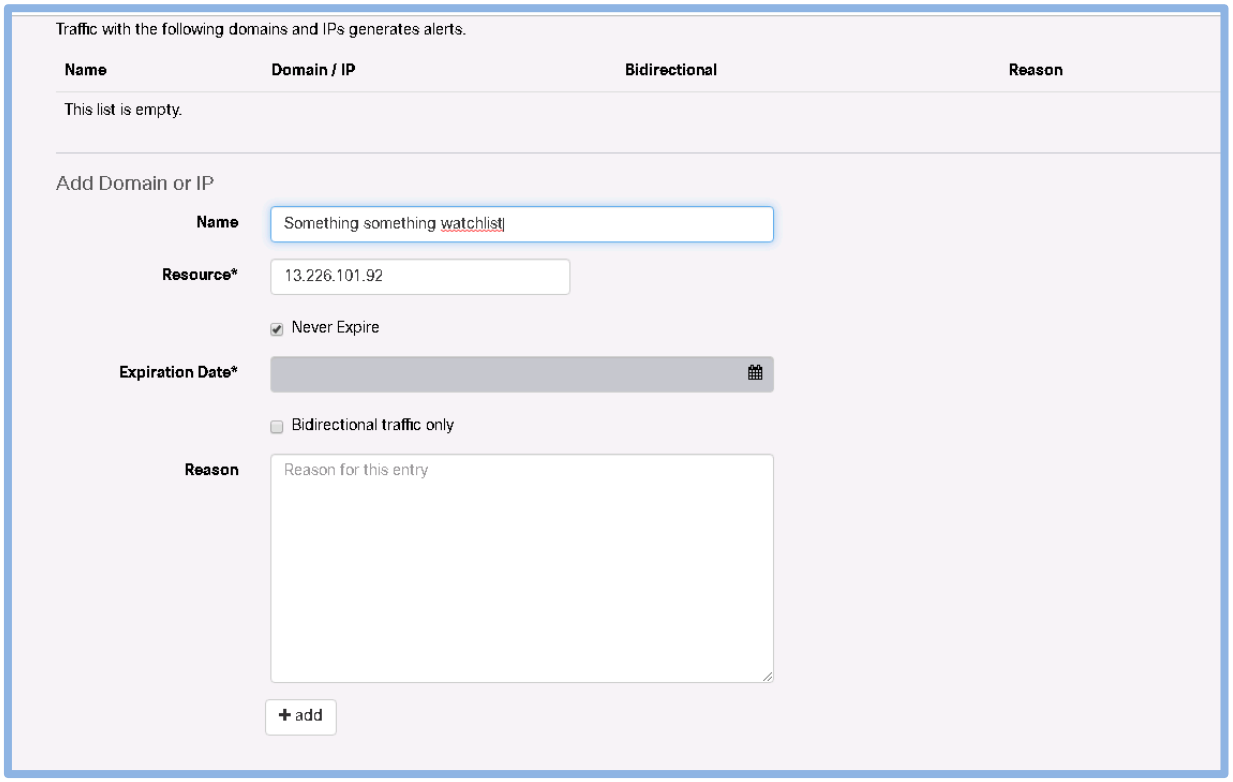


Figure 40. Custom IP watchlist

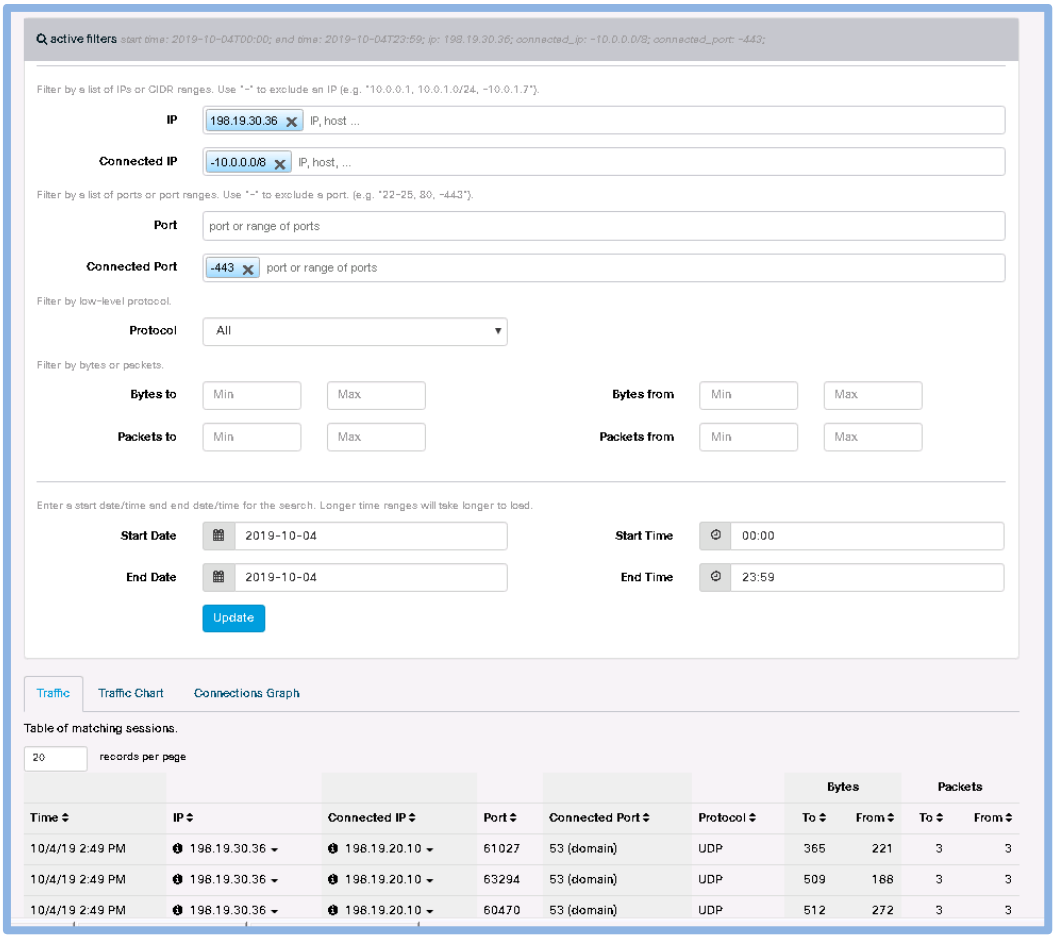


Finding Flows using Session Filter

1. Go back to Models > Session Traffic from the menu bar.
2. Previously we just searched for 443 traffic. What if we wanted to search all flows except 443? In the session filter you can put a minus sign before the port or IPs to remove a certain criterial from the flow report.

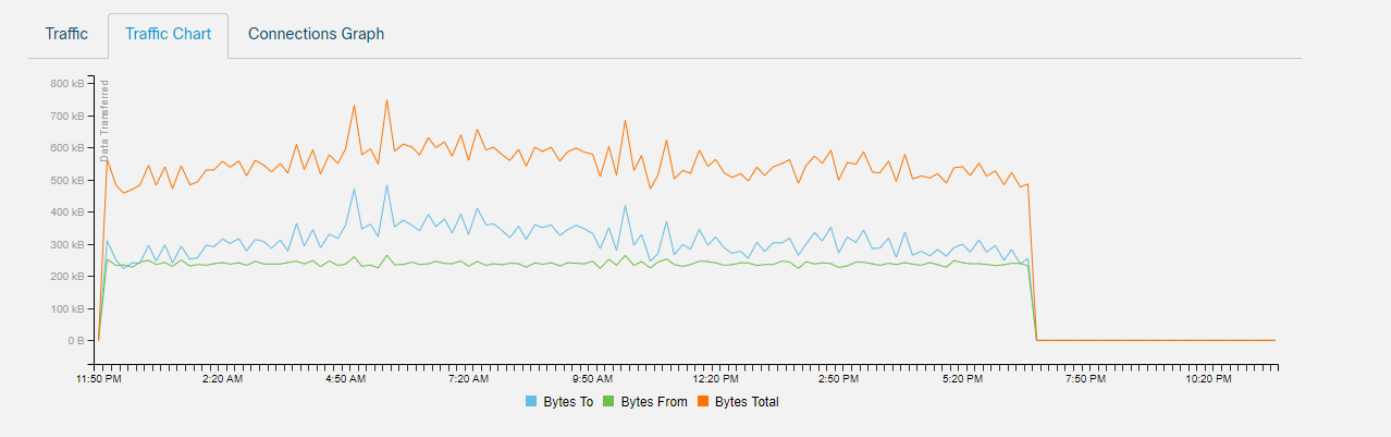
   Enter the sensor IP address of 198.19.20.143 into the IP field. In connected IP enter -10.0.0.0/8. In connected port enter -443. This query will show all flows that are NOT to an IP in the 10.0.0.0/8 CIDR range. It will also remove any flows to port 443 from the query. Select Update to run the new query and verify the results.

Figure 41. Custom Flow Query



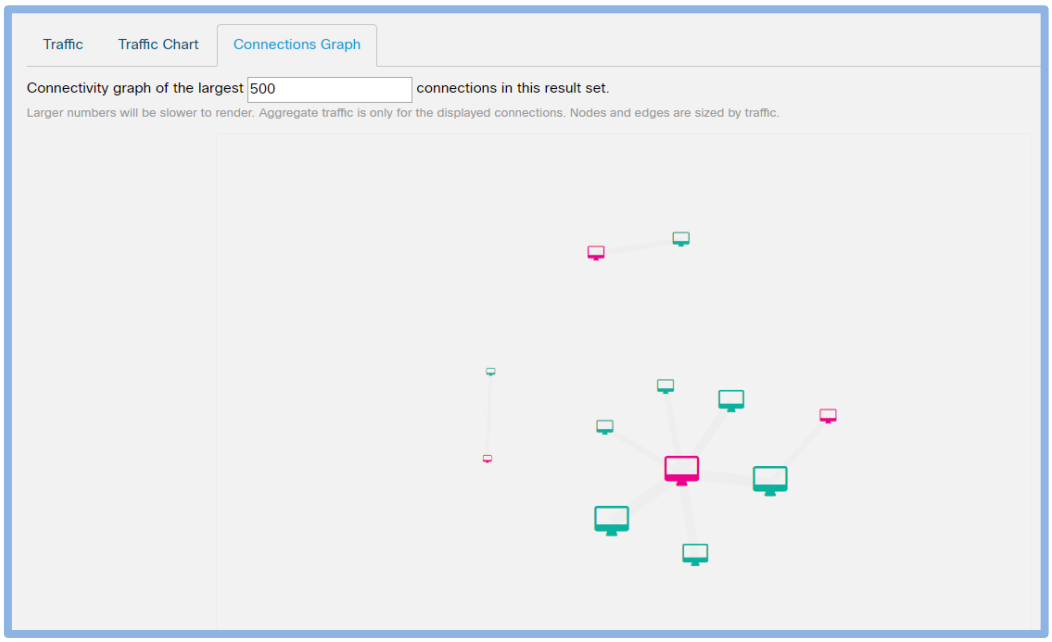
3. Next, select Traffic Chart. This will graph the flow traffic so you can more easily understand the volume and if needed narrow the query. It can be difficult to analyze many lines of flows to find the interesting behavior, traffic chart and connections graph a good way to visually see the data.

Figure 42. Flow Query Traffic Chart



4. Next, select Connections Graph This will show machine connectivity for the flow query ran. The larger the icon the more traffic was sent to/from it. Click on an icon to see IP address and traffic amounts. You can zoom in using your mouse.

Figure 43. Connections Graph

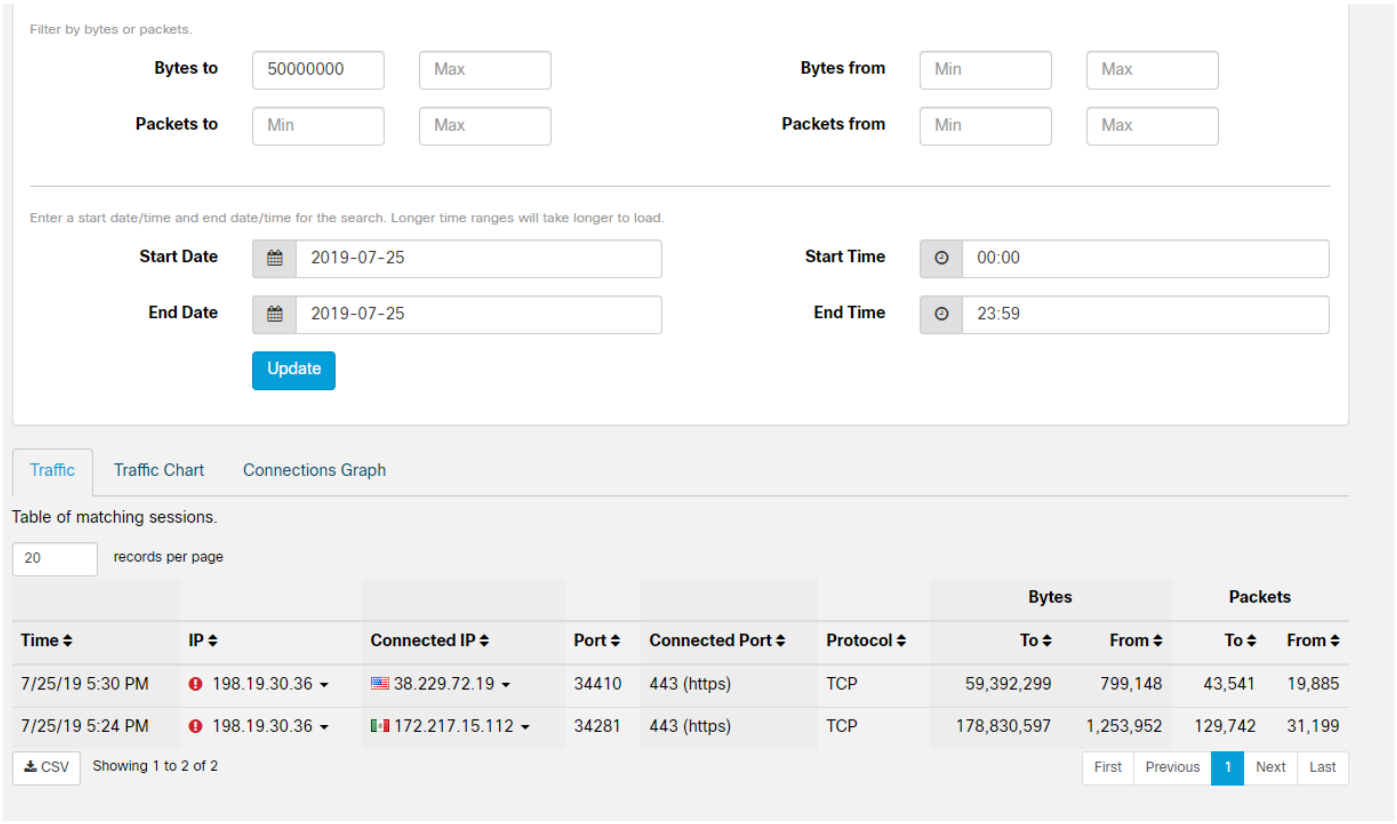


Finding Flows for the TOR download

1. By now the TOR download should have uploaded to the portal. Start a new session traffic search, in the Bytes to Min field, type 50000000 to filter the results to only display flows that were greater than 50 MB of data exchanged, shown below

2. Scrolling through the flows you should see a flow between your Workstation 1, 198.19.30.36, as the subject connected to an Internet facing peer.
1. In the search below, the ~59 MB download was with 38.229.72.19 out of the US over https. Note: The peer IP address may be different from when you downloaded your Tor executable.
2. Notice the MB size coming down from the peer to your Workstation 1.
3. Click the black triangle next to the external IP address to see more context about it or perform additional searches.

Figure 44. Flow Table Quick view

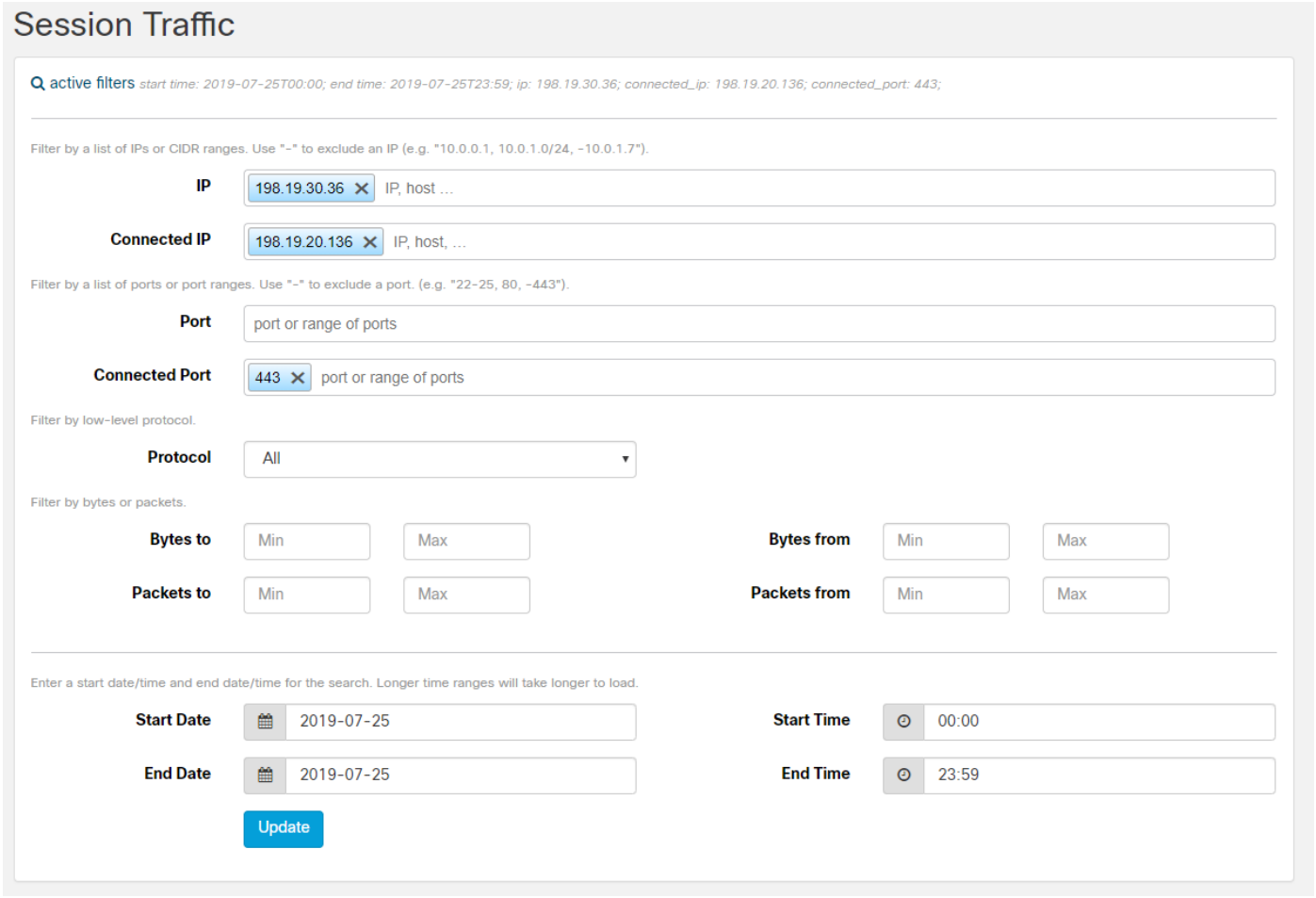


Filter the flow table by one of the Foreign IP addresses with :443 you saw in the netstat lab.

1. Remove the 50000000 value we added earlier in Bytes to
2. In the Connected IP field enter an IP address you observed in your netstat lab above. The IP address may vary from what is listed in the figure below.

Peer IP Address Filter

Figure 45. Session Traffic



Summary

In this Getting Started lab, you:

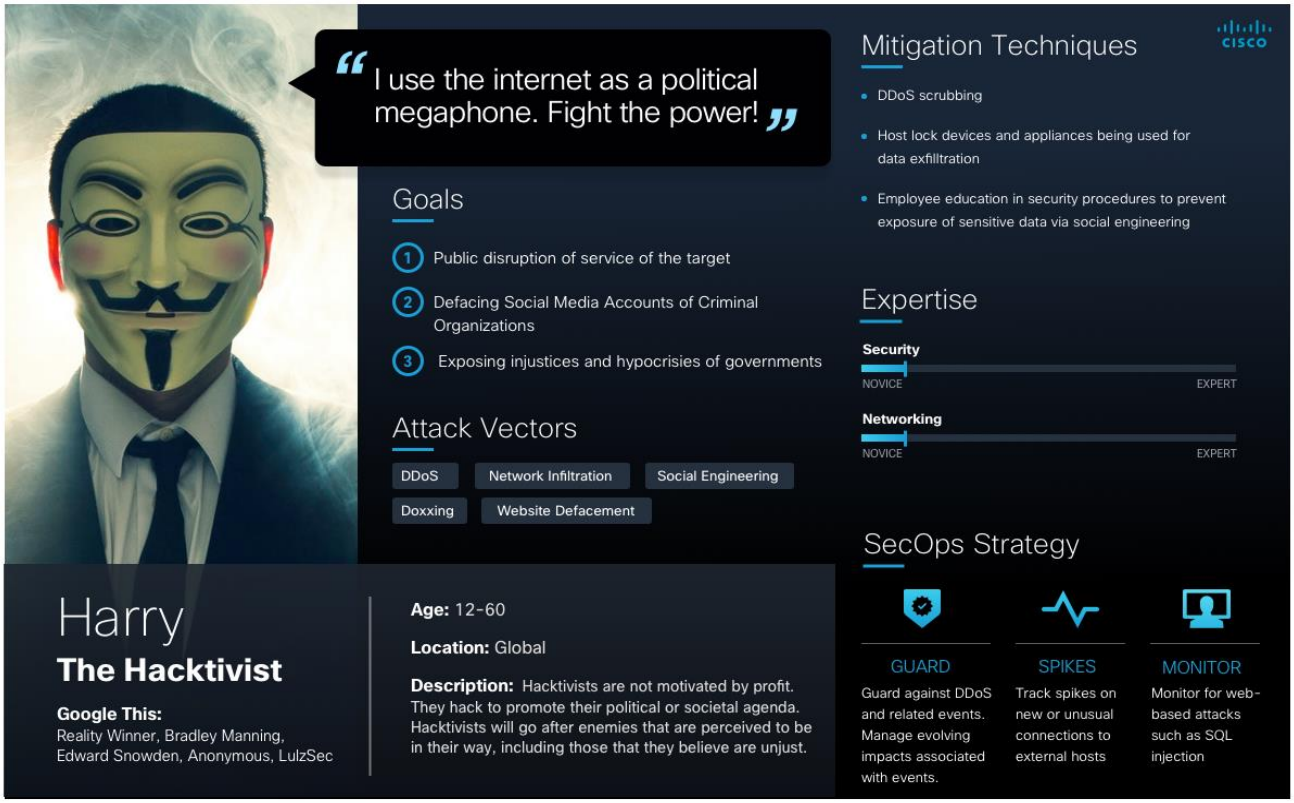
- Became familiar with your Workstation that you connected to in the data center
- Learned that all network conversations are accounted for from this machine through NetFlow collection
- Learned how to run a basic Flow Search in Stealthwatch Cloud to see all https flow between your Workstation and the Internet.

- Understood some basic Stealthwatch Cloud configuration features

☑ End of Lab: Please pause here.

Breach Detection

To help get in the mind of an attacker, take a minute to read through the persona of “Harry the Hacktivist” and how he operates. Understanding the attacker can help build solutions to defend your organization.



Lab 1: Remote Access Breach using stolen credentials

Business Objectives

According to the Ponemon Institute 2017 Cost of Data Breach Study of 419 companies in 13 countries, $3.62 million is the average total cost of a data breach. To help combat this, it is critical to try to account for 100% of network conversations to detect threats that bypass traditional monitoring solutions.

Test Drive Objectives

In this test drive, you will see first-hand the importance of capturing flow data from as close to the endpoints as possible to be able to account for all active and historical network conversations.

Test Drive Requirements

- Stealthwatch Cloud Portal

Test Drive Outline

Task 1. Connect to a server running Remote Desktop within a datacenter

Task 2. Download an exploit-kit

Task 3. Perform network scanning reconnaissance

Task 4. Install exploit-kit

Task 5. Investigate Security Events generated in Stealthwatch Cloud

Task 1: Connect to a Remote Desktop server within a data center

Below is a list of realities of why you need to build stronger defenses beyond access control lists or firewalls:

- Firewalls are as good as the person implementing them, mistakes happen.
- If the access control policy is misconfigured and an any-any rule is moved to the top, how would you detect this before it's too late?
- Detect threats when an authorized server is used with stolen credentials.
- Account for all traffic on the inside of the firewall so you can build a general ledger of both authorized and non-authorized traffic making it through the firewall and provide a second chance detection.

Scenario: You have been performing reconnaissance against an organization and have identified a remote desktop server that is exposed to the Internet. You have discovered the below credentials to the server and begin building a foothold inside the organization. In this lab, you will need to access Workstation 1, which gives you access to all data center resources.

Note: If Remote Desktop is already up, move to Task 2.

Click Remote Desktop link to launch a web Remote Desktop session built within dCloud shown below.

Note: Username: wkst\Administrator Password: C1sco12345

Figure 46. Workstation1 Remote Desktop

You are now inside the organizations data center by leveraging a server exposed to the Internet and using stolen credentials!

Task 2: Download an exploit-kit (this was already done previously)

The exploit Kit is located in the downloads/lab-swc directory

Task 3: Perform network scanning reconnaissance

One of the first phases of any attack is reconnaissance. Various open source tools are available to attackers. In order to break the Cyber Kill Chain, tools must be able to identify when this type of attack is occurring.

In Task 3, we will assume the attacker is already in the network, selecting targets through scanning activity, and attempting to identify vulnerabilities in the target network.

Perform these steps to initiate an attack against the target network to identify additional resources in the data center.

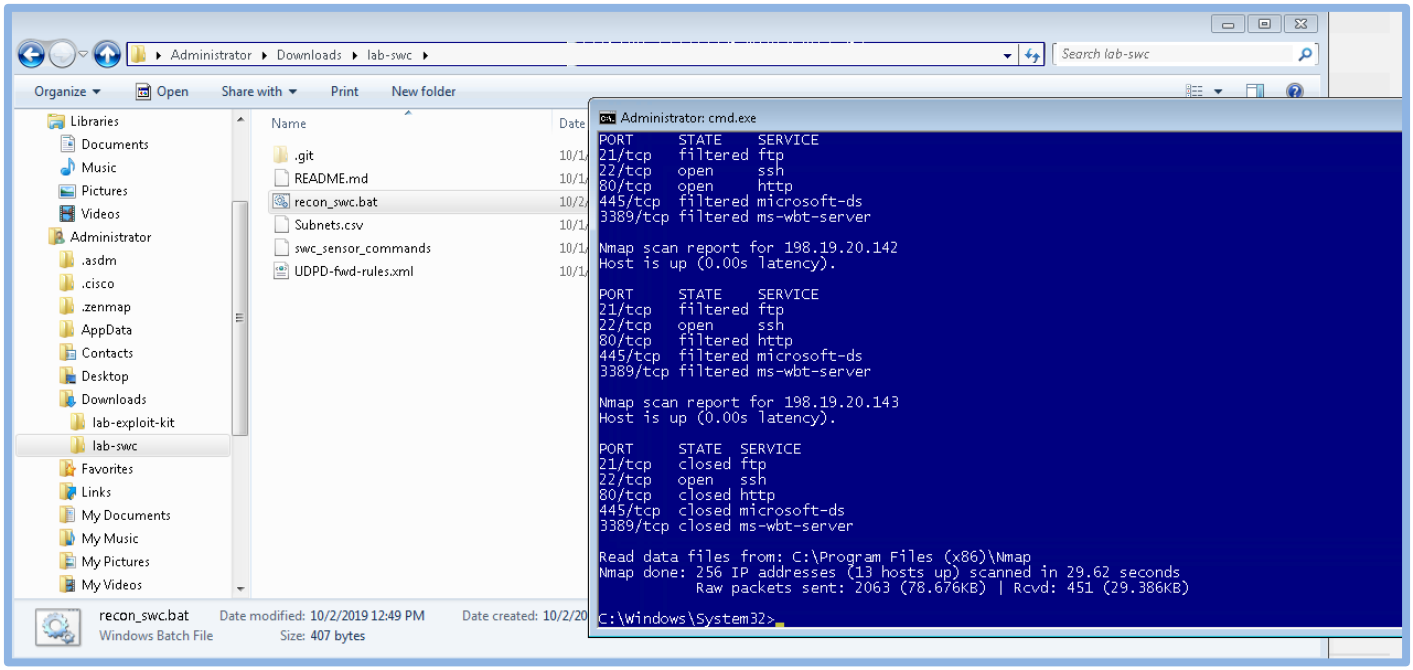
From the Remote Desktop session of WKST1 in the dCloud lab:

1. Open the lab-swc folder that was downloaded from GitHub within the Downloads directory.
2. We are searching for common management ports such has 22 = ssh, 23 = telnet, and 3389 = Remote Desktop, etc.. Run the recon_swc.bat as illustrated below to perform reconnaissance and find other devices within the network.

3. The recon.bat will pause so you can see the below nmap scan is what is running. Press any key to continue the scan.

   nmap -n -v -p 21,22,23,25,80,443,3389 10.201.0.0/24 198.19.20.0/24 --disable-arp-ping

Figure 47. nmap scan



Note: The scan could take over 5 minutes to complete. When complete, you will see results similar to those shown in the screenshot below.

Make note of the number of hosts scanned and scroll through to see what hosts are listening on given ports.

What does this command mean?

-n: Tells Nmap to *never* do reverse DNS resolution on the active IP addresses it finds. Since DNS can be slow even with Nmap's built-in parallel stub resolver, this option can slash scanning times.

-v: verbose meaning show the contents on the screen.

-p: Port scan on multiple ports. In this case ports 22, 23 and 3389

--disable-arp-ping: Nmap normally does ARP or IPv6 Neighbor Discovery (ND) discovery of locally connected ethernet hosts, even if other host discovery options such as -Pn or -PE are used. To disable this implicit behavior, use the --disable-arp-ping option.

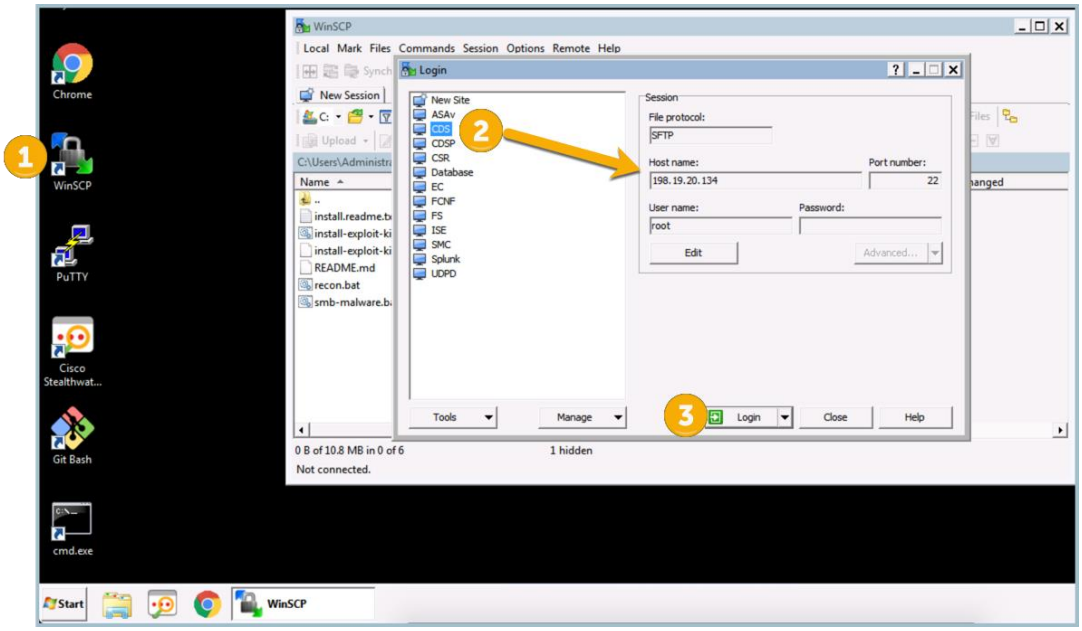
The default behavior is normally faster, but this option is useful on networks using proxy ARP, in which a router speculatively replies to all ARP requests, making every target appear to be up according to ARP scan.

Task 4: Install exploit-kit

Let's SCP and install the exploit-kit on one of the servers identified during the network scan.

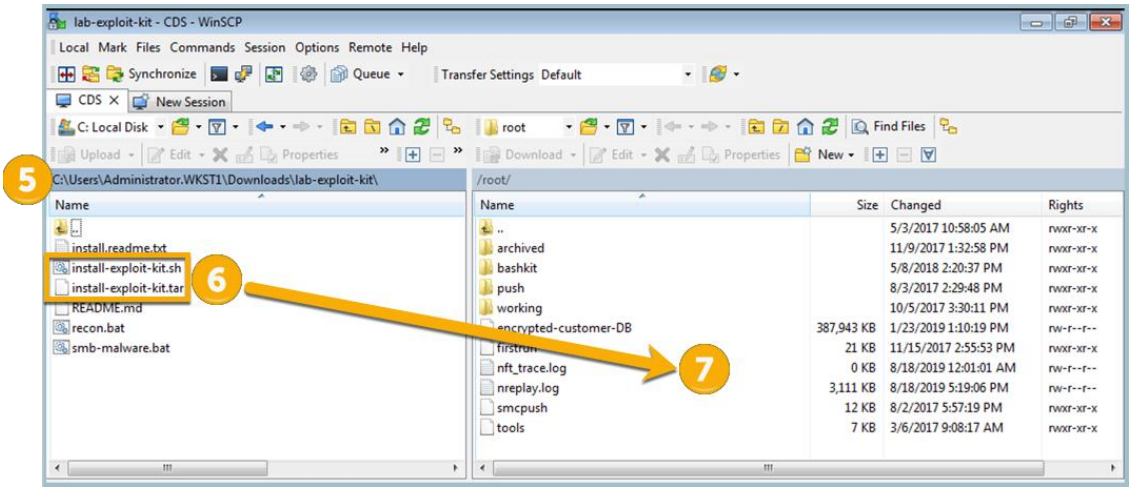
1. Open WinSCP from the Desktop as shown below. Note: If an update appears, ignore the update.
2. Select CDS, as shown below.
3. Select Login, the password is pre-saved.

Figure 48. Login WinSCP



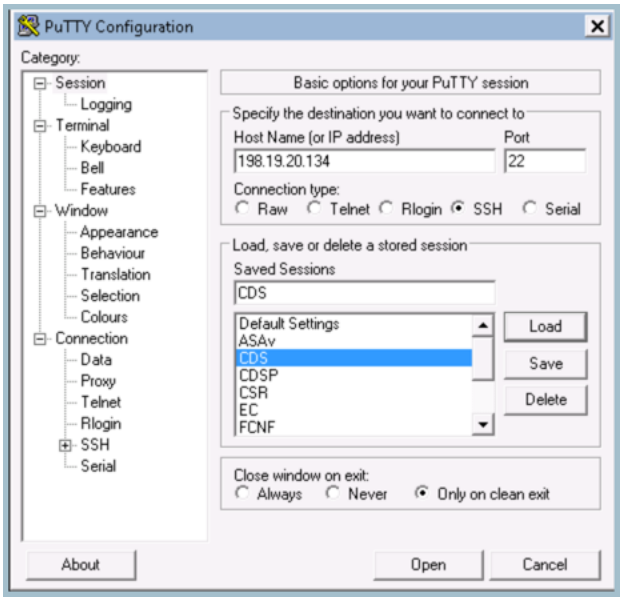
5. Within the left panel of WinSCP, browse to c:\Users\Administrator.WKST1\Downloads\lab-swc\lab-exploit-kit on the left-hand navigation pane, as shown below.
6. Highlight install-exploit-kit.sh and install-exploit-kit.tar
7. Drag and drop install-exploit-kit.sh and install-exploit-kit.tar within root in the right pane, as shown below.
8. Close WinSCP when the transfer is complete.

Figure 49. WinSCP



9. Open Putty located on the Wkst1 desktop and use the CDS session to SSH into 198.19.20.134 (which is the server we installed the exploit-kit on) with username of root.
10. Enter the password C1sco12345 when prompted in the Putty session window.

Figure 50. Putty

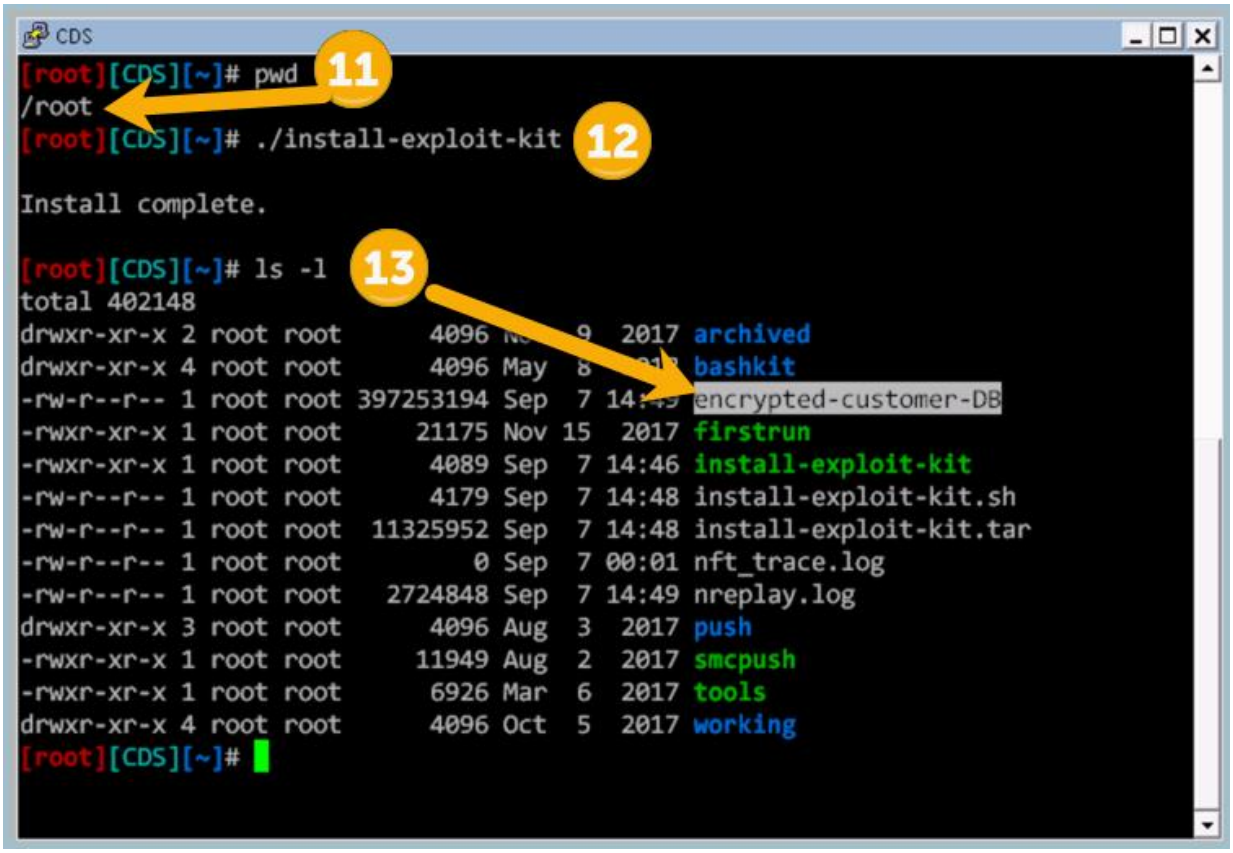


11. Once logged in, enter pwd (preset working directory) to make sure you are in the root directory. This is where you placed the exploit files.
12. Run the following command ./install-exploit-kit as shown below to install the tools used to create a foothold within the organization. This command is also listed in the

wkst1_command.text file used previously. Ignore the errors, we bought this exploit kit on Amazon and it only had a 3 star rating.

13. Run ls -l and make note that the exploit kit has captured a customer database with the name encrypted-customer-DB. You can exit out of the SSH session.

Figure 51. WinSCP



Task 5: Investigate Security Events Generated in Stealthwatch Cloud

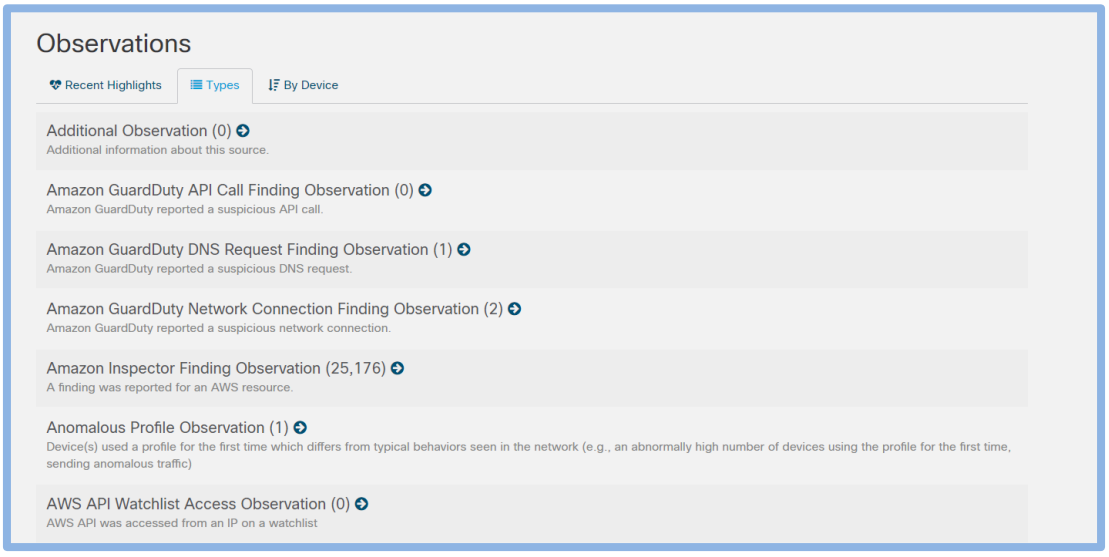
Stealthwatch Cloud will have stored flow records for all north-south connections and east-west connections to the Remote Desktop server and detected the attack traffic that was initiated in the previous lab.

1. Login to the Stealthwatch Console if not already logged in. There can be up to a 30 minute delay between when events happen in the network and when they appear in the Stealthwatch Cloud portal, while the recent flow data is processed, we are going to review some other features of Stealthwatch Cloud

2. Observations are the building blocks for alerts in Stealthwatch Cloud, they can be thought of simply as facts about the network devices or users that can be classified. As traffic is observed and patterns are detected they are tracked as an observation, over time these being to tell us about the behavior of a user or machine. Stealthwatch Cloud has approximately 75 Observation types ranging from ones focused on public clouds like AWS & Azure or more generic ones that identify network heartbeats, watchlist interactions, traffic outliers, and more. An Observation should not be considered an alert, rather they feed into our entity modeling engine to produce alerts for known bad behavior (e.g. scanning) or to detect behavior deviations that indicate something should be investigated.

   Go to the Observations tab in the Stealthwatch Cloud portal, you will see three tabs below it, Recent Highlights, Types, and By Device. Click on Types to see the various Observations that Stealthwatch can detect. They are listed in Alphabetical order, you will notice may are not limited to network traffic.

Figure 52. Observation List

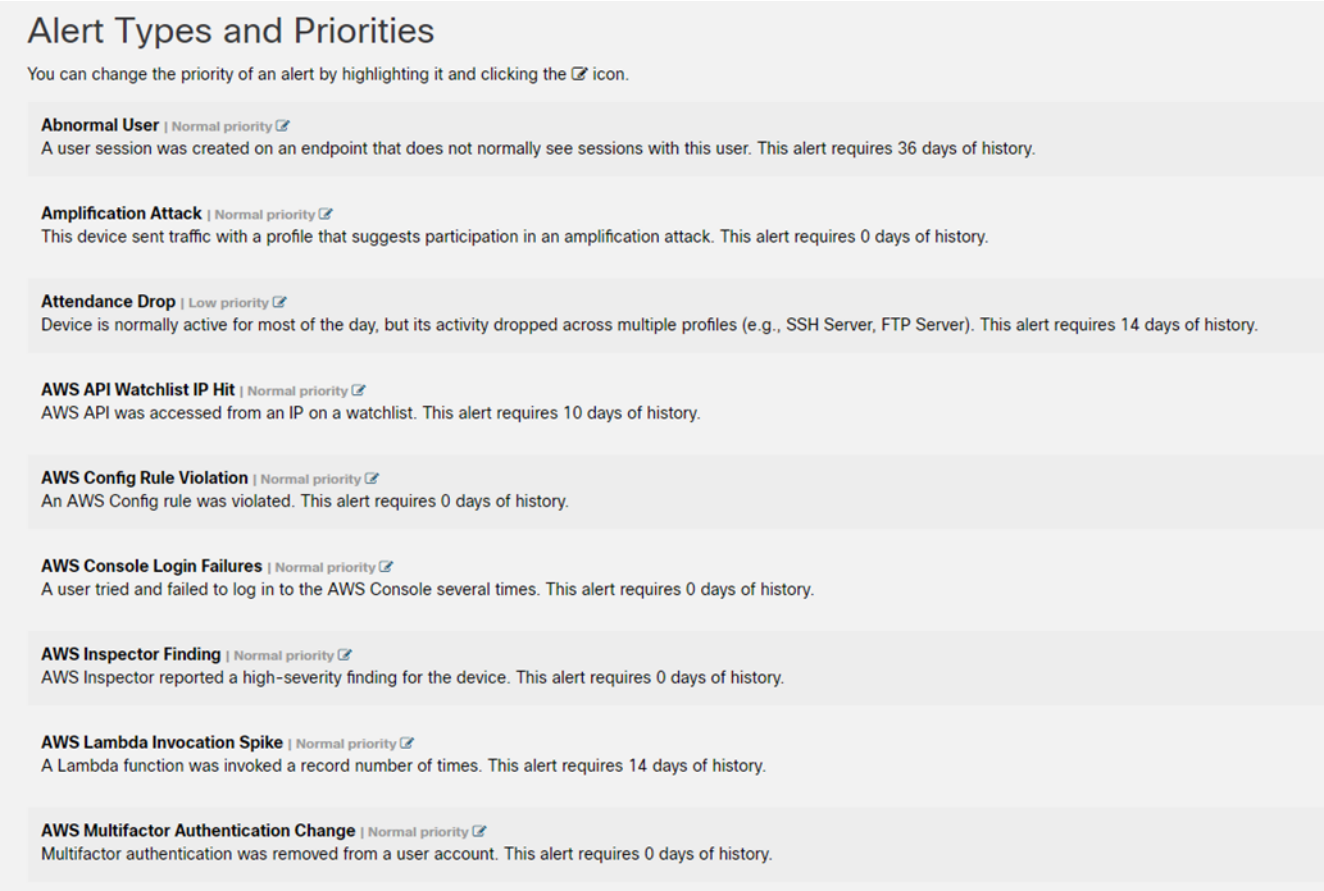


Selecting By Device, will sort all the network endpoints by Observation count. This can be useful to see what hosts might need to be looked at in more detail. Since our portal is new this is most likely blank but will begin to fill in. Below is an example of what a normal view would look like.

Figure 53. Observations By Device

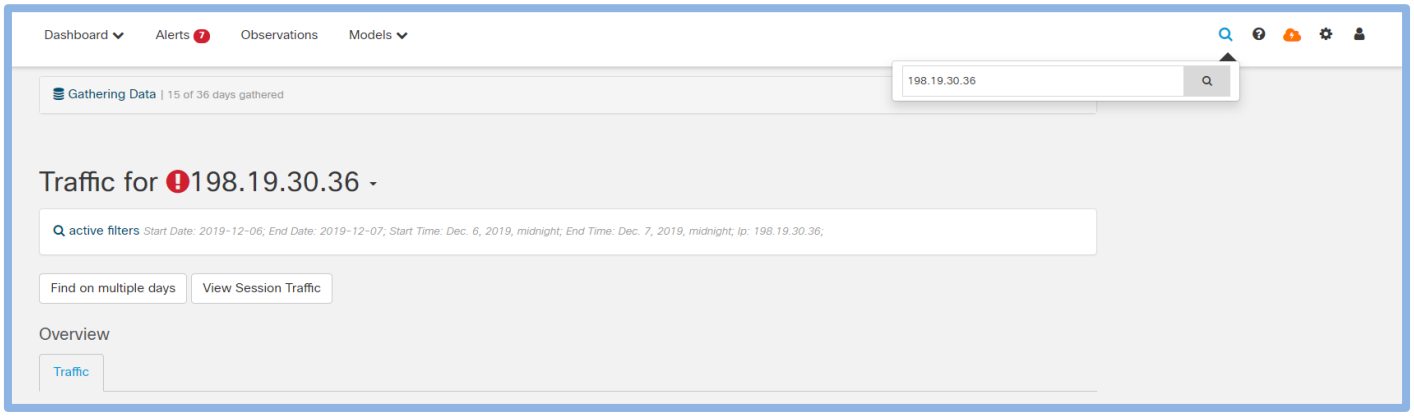
3. Go the settings Icon, then Alerts, then select Configure Alert Priority to see the various types of alerts that are included with the service. Notice how each have a historical data requirement, the longest baseline for Stealthwatch Cloud is 32. The majority of the alerts built-in and will auto enable after hitting their baseline period, others such as the User Watchlist Alert would only generate if a user configured a watchlist such as we did earlier with the TOR network.

Figure 54. Alerts Menu



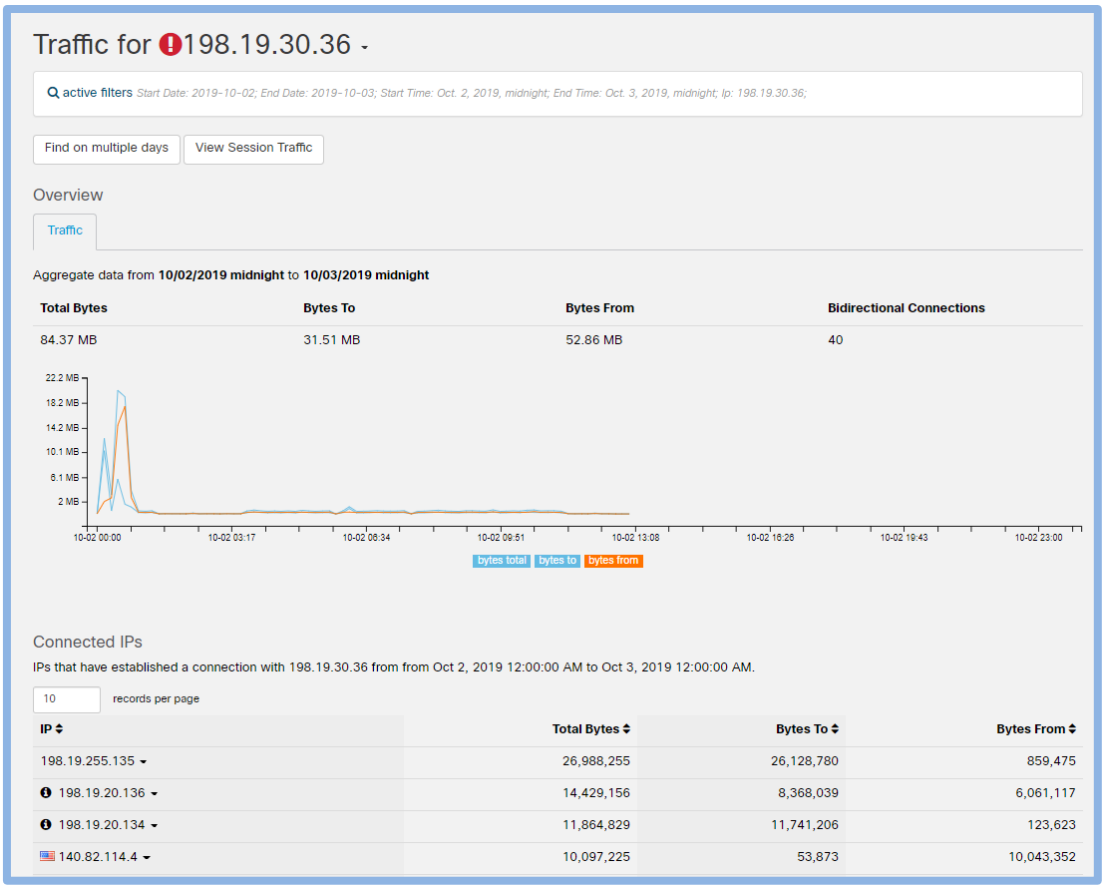
4. Let's look more at our workstation, type the IP address of Wkst1 in the search window, by selecting the magnifying glass in the upper right hand of the portal and typing in 198.19.30.36.

Figure 55. Search Window



5. You will see a summary of the recent IP connectivity. View the top Connected IPs and Ports.

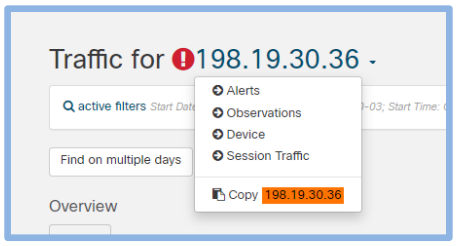
Figure 56. Host Traffic Report



6. Next, we will look at the Observations for this machine. Use the black triangle to pivot to Observations.

   For this host you should see some initial observations such as watchlist hits and remote access connections, this will continue to grow as we collect more traffic.

Figure 57. Observations Pivot



7. Check to see if there are any alerts for Wst1. Go to the Alerts menu in the Stealthwatch Cloud portal to see if any alerts have published. Likely you will see one called "User Watchlist Hit" for the interaction between the workstation and the TOR network, soon you should also see one called "Internal Port Scanner" that will have details on the recon file we initiated earlier. If you don't see them, then it could be still be a delay in processing. Continue to look back at the alerts.

Figure 58. Alerts Menu

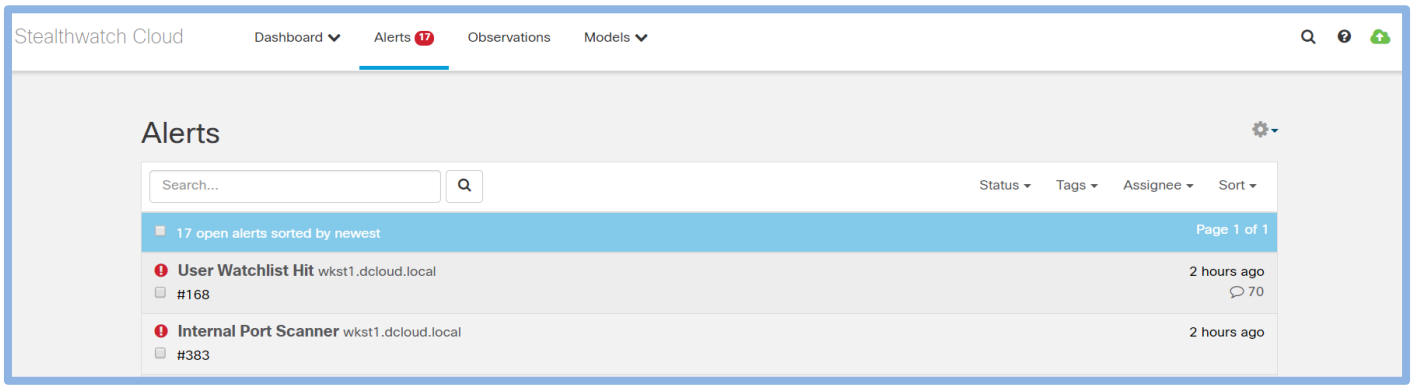
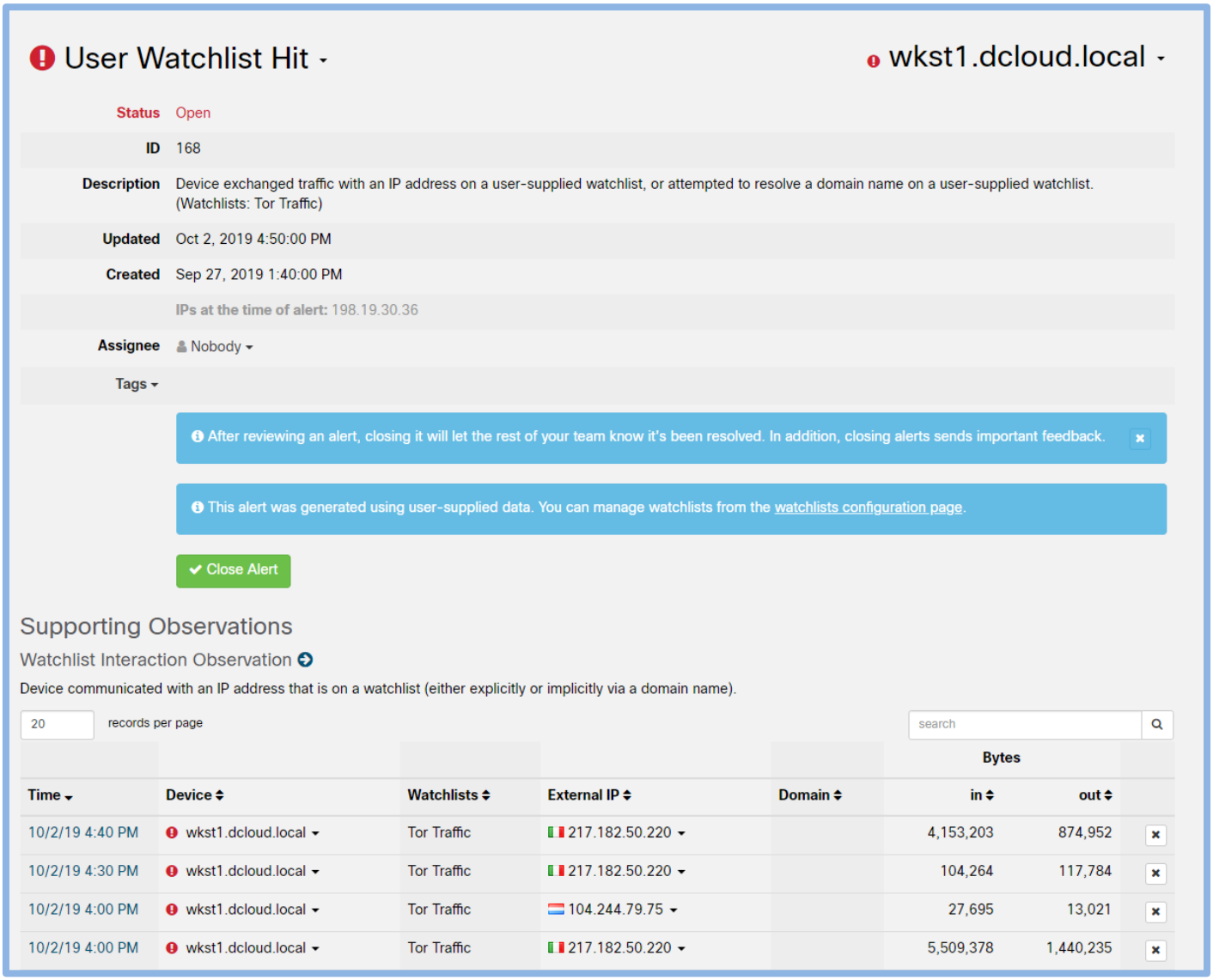


Figure 59. Watchlist Alert

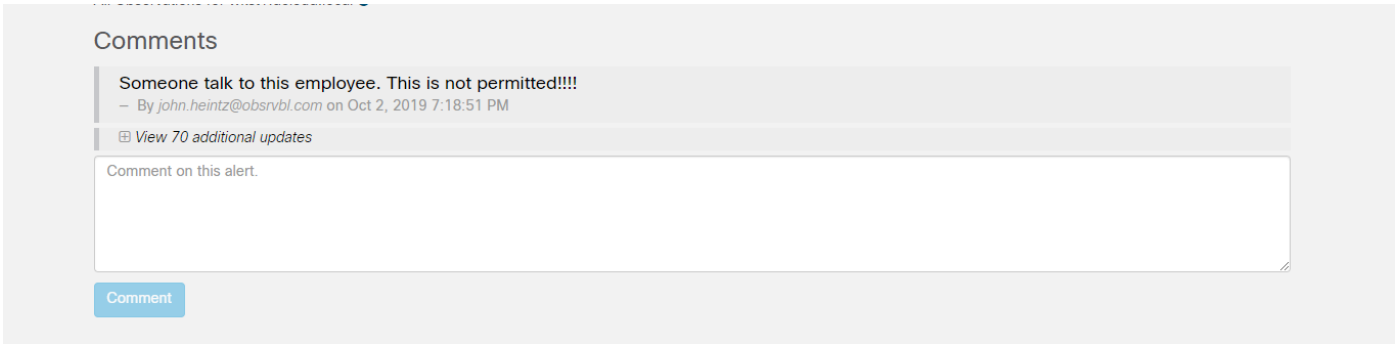


Open the User Watchlist hit alert, investigate the following sections within the Watchlist alert for wkst1.dcloud.local as shown below.

1. You will notice the Supporting Observations or “evidence” for why the alert was fired. As this host continues to communicate with TOR, the IP flows will continue to update.
2. Users may have several Watchlists that are active, the Observation details will reference the specific list that was defined. The external IP will show the flag of the country that it was Geo-coded to. Additionally, the Observation will summarize the traffic in 10-minute periods.
3. Click on the time-stamp to see more details on the supporting flows.

4. As part of the Alert workflow, users can add comments. Add a comment for the User Watchlist Alert. These will remain attached to the alert, alerts are kept in the Stealthwatch Portal as long as the service is active.

Figure 60. Alert Comment



5. If the port scanner alert has triggered, open it and look at this Observations as compared to the Watchlist alert. Click the timestamp to see all the flows that were used for that alert. Try closing the alert to see how Stealthwatch Cloud prompts for user feedback so we can ensure alerts provide value to our customers. If it has not generated yet, come back after the next lab.

Figure 61. Internal Port Scanner

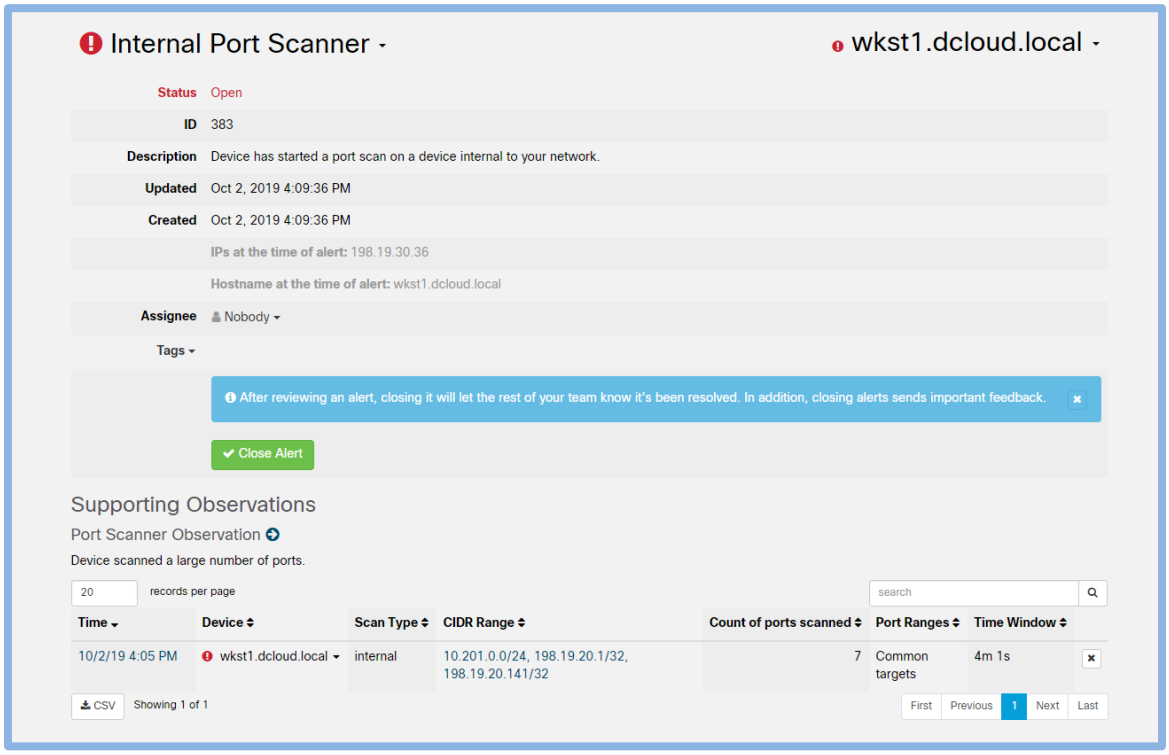
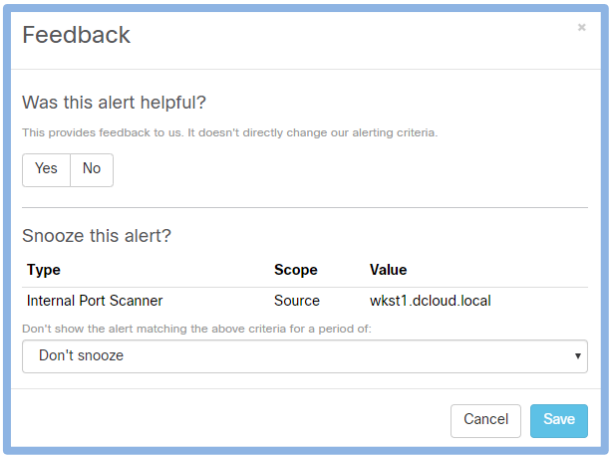


Figure 62. Alert Feedback



Summary

Within this test drive you learned:

- How to investigate an alarm
- How to investigate a host
- How Observations are used to detect network or user events and create alerts
- How to review Stealthwatch for alert and Observations

Lab 2: Historical Traffic Analysis to Identify Threats from Suspect Countries

Business Objectives

Threats are hiding in legitimate network traffic through common web browsing or through ports and applications that are trusted within firewall rules and on the endpoint. One way to identify these threats is to account for all network traffic entering and leaving the organization to the Internet. Once this visibility is collected, retrospective analysis over this long-term history can be performed to identify what should not exist. Through this visibility and retrospection, detection of threats will be improved along with being able to improve enforcing network segmentation.

Test Drive Objectives

Within this test drive you will gain an understanding of the importance of accounting for all traffic entering and leaving your organization to the Internet to identify threats hidden within trusted connections.

Test Drive Requirements

- Stealthwatch Cloud Portal

.

Test Drive Outline

Task 1. Generate traffic to random countries.

Task 2. Identify traffic to random countries.

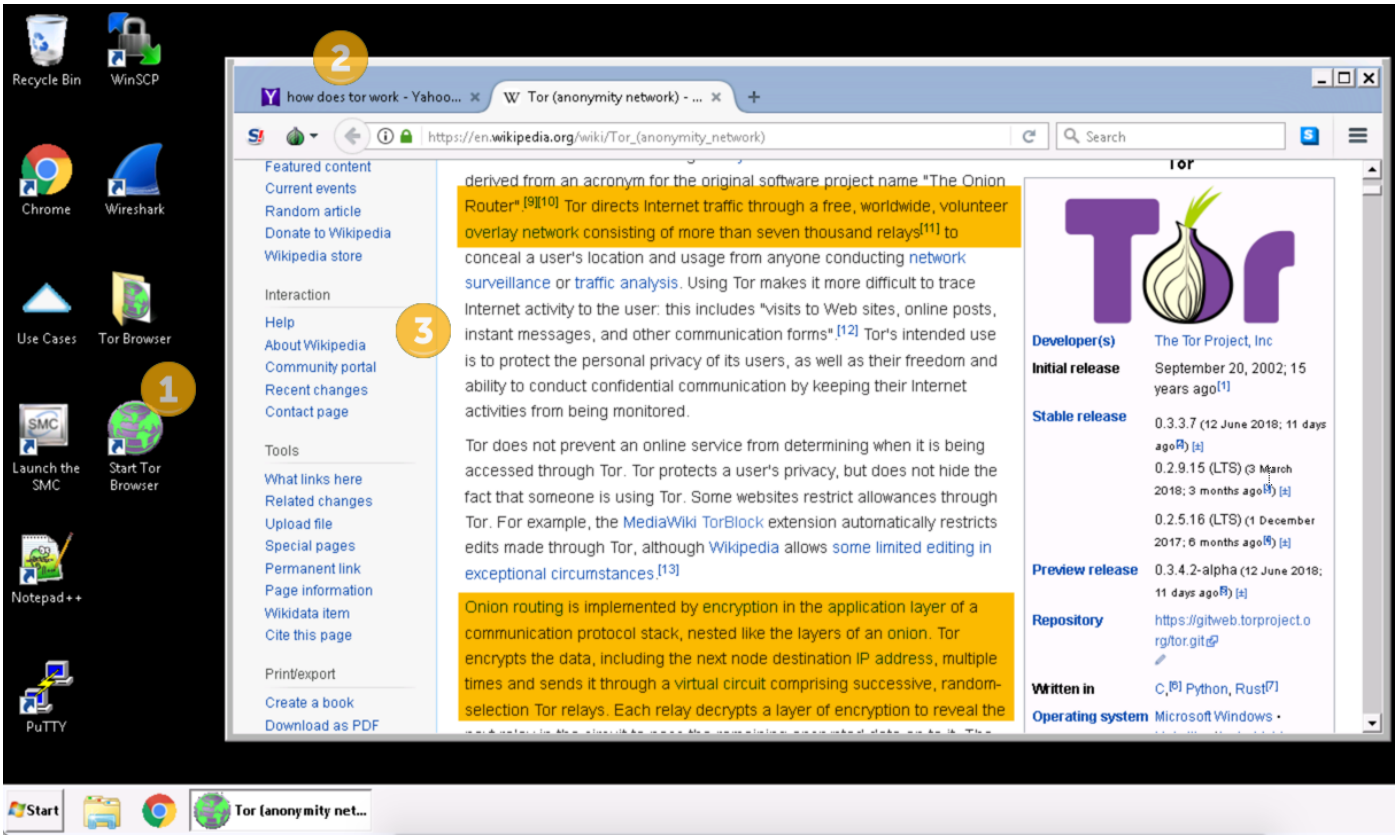
Task 3. Identify what alerts are activated for high risk countries

Task 1: Generate traffic to random countries

Within this section you will generate random traffic that is trusted from an installed application over common ssl web traffic.

1. Click Start Tor Browser from the desktop of the remote desktop Workstation 1.
2. Navigate to yahoo.com to (if you are redirected scroll down to the bottom and accept the Yahoo privacy agreement) begin generating web traffic and click on a few articles. Yahoo.com is being recommended as the search engine as it contains many widgets that generate more web connections to different sites. After browsing through a few articles to generate traffic, search for "how does tor work".
    a. Note: Browsing with TOR can be very slow by nature
3. Open and read the Wikipedia article shown below on how the Tor network works.

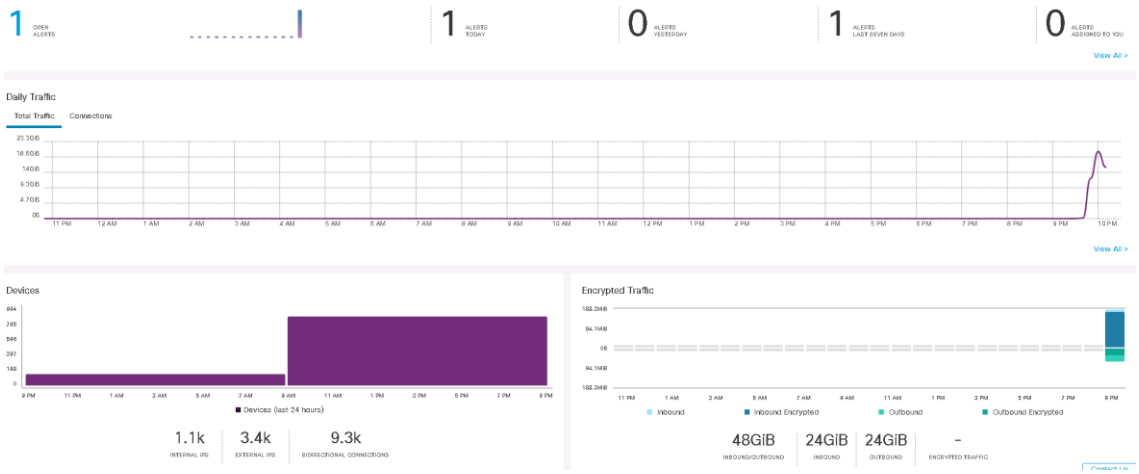
Figure 63. Search within the Tor Browser



Task 2: Investigate traffic to random counties

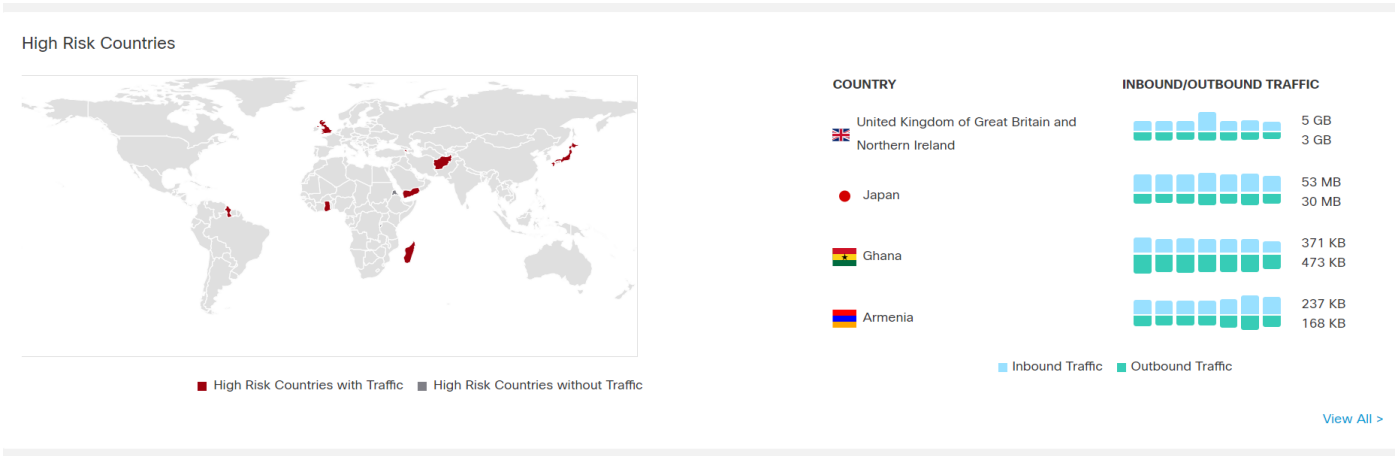
Within this lab you will learn how to view all countries your Workstation 1has connected to.

1. Open the Stealthwatch Cloud portal and login
   2. Select Dashboard, then Network Dashboard, your portal will start displaying details about the network activity, such as traffic, connections, encrypted traffic, etc.



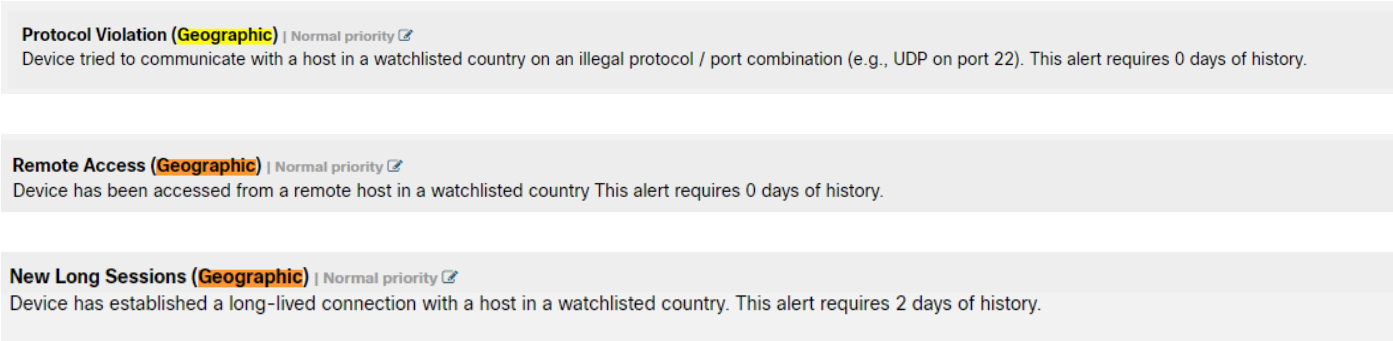
   3. Stealthwatch Cloud Geo-locates any IP that a device communicates with, it will track the traffic to countries you designate as high risk. This page summarizes the country activity.

Figure 64. Country Heat Map

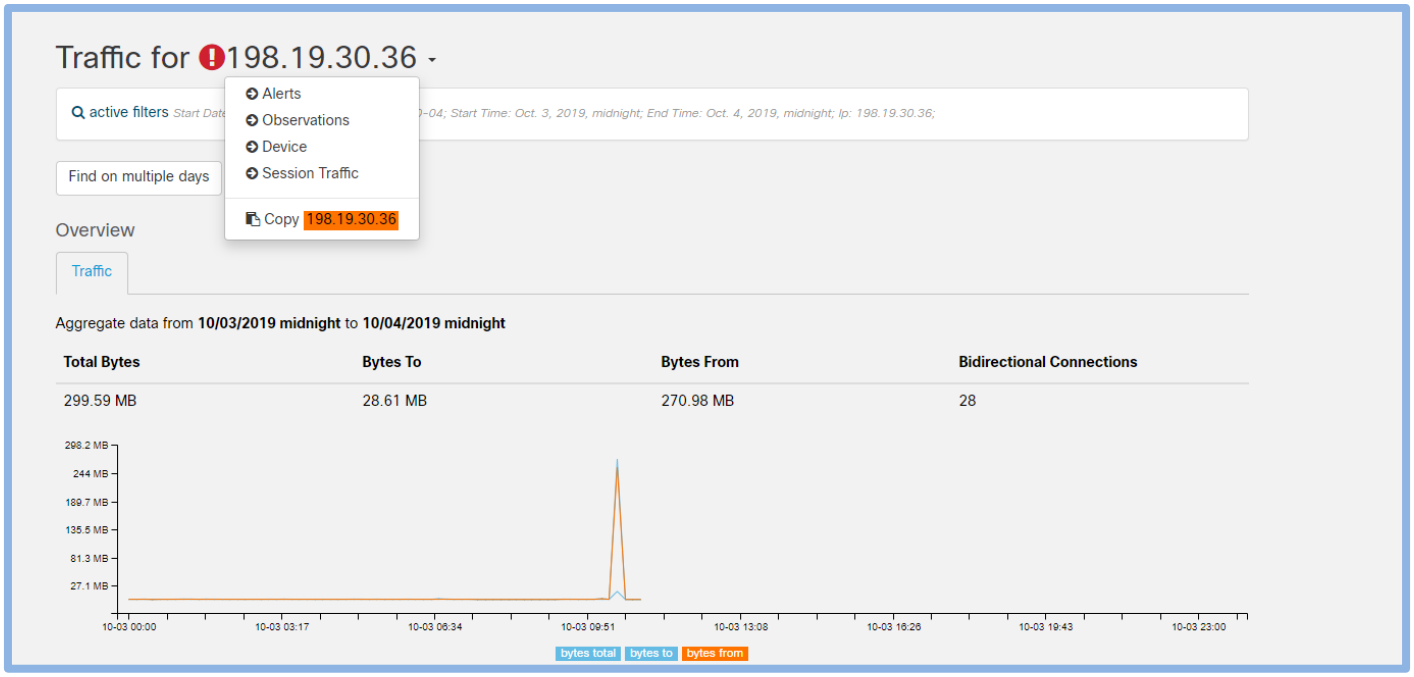


4. Select the settings Icon, then Alerts, then Configure Alert Priority. Do a Ctrl+F to run a search on this page for “Geographic”, this will list any Geo based alerts. Three alerts are associated with the Country Watchlist.

Figure 65. Country Watchlist Alerts

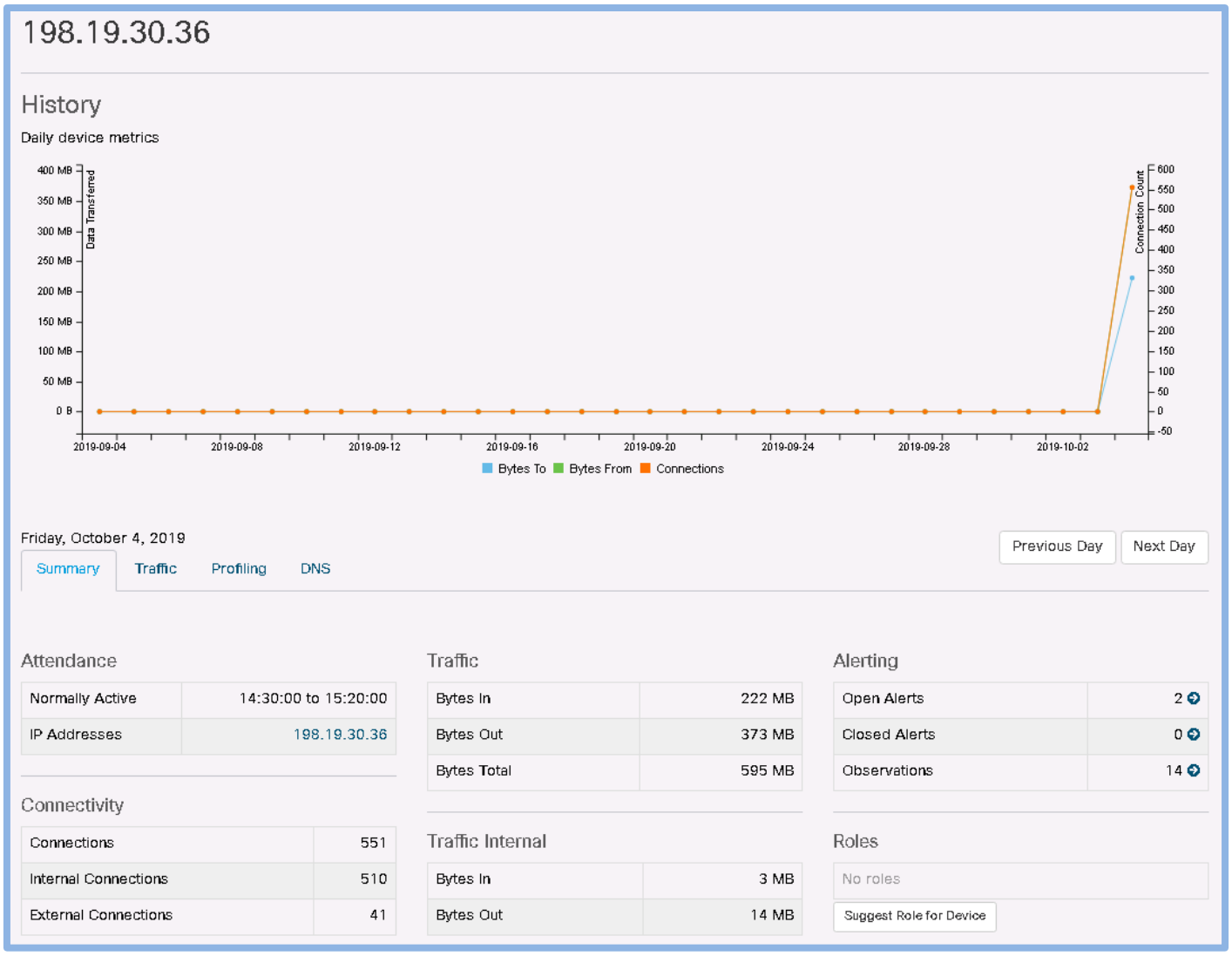


5. Let’s now look the countries that WKST1 has communicated with. Select the hour glass to search for IPs in the portal. Enter 198.19.30.36 to pull our workstation.
6. Select the triangle next to the IP address and then Device

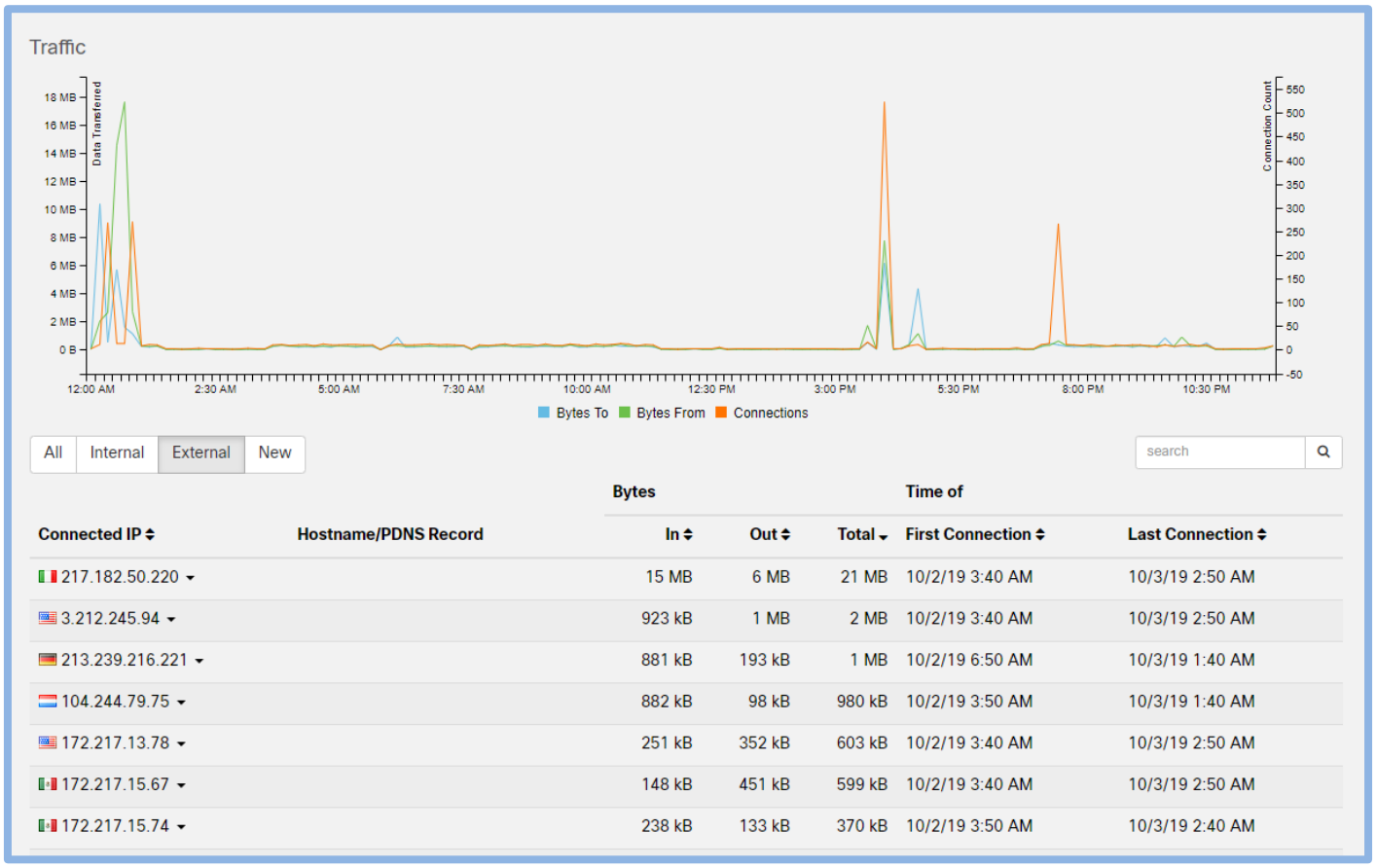


7. This initial device page summarized connectivity for a given day such as Internal and External Connections, Traffic Profiles sorted by byte count, etc. Since this is a new system there is not history prior to today. We also don't have a role detected yet since we have not seen enough traffic to say for sure what kind of roles the device is part of.

Figure 66. Device Summary View

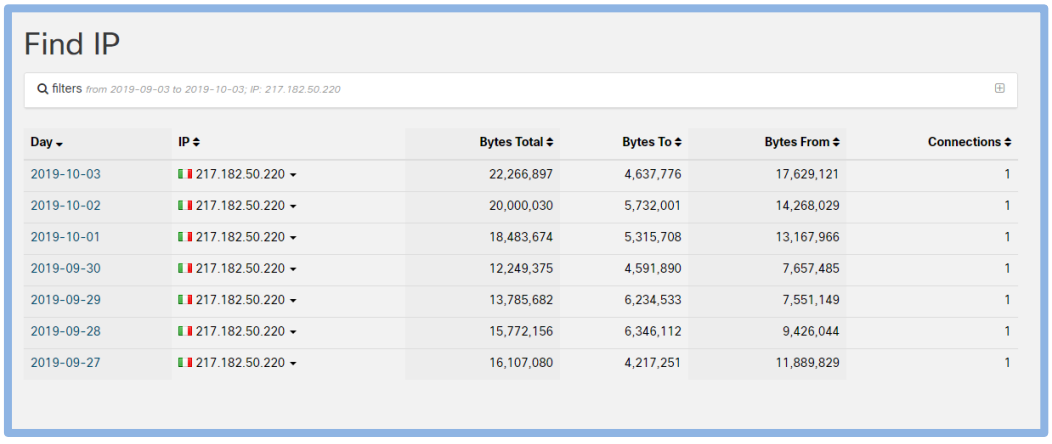


8. Next select the traffic tab. This page will show detail about the internal and external communication for a specific day. Select External to see all traffic to IPs not listed as local subnets. You can sort by Bytes and Connection time.



9. To see more details and options about an external host, select the triangle next to the IP address. For example, you can see all traffic to that IP across any IP address in the portal by selecting find IP on multiple days.

Figure 67. Traffic Report for External Host

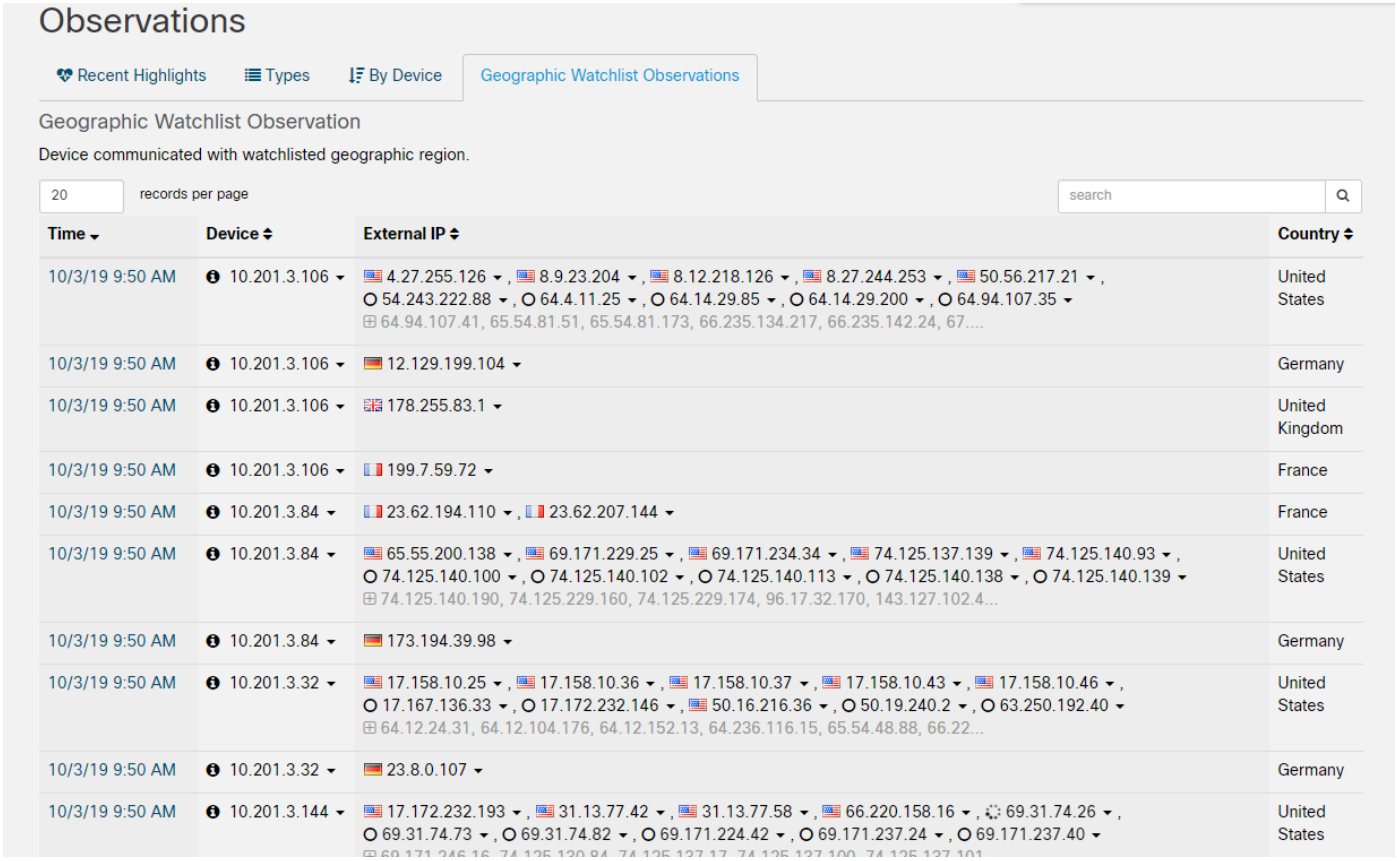


10. Select Profiling which is the next tab in the device view. This shows the connections by type of application, for Wkst1 the top application by traffic is RDPServer but since it only has one connection it a small part of the pie chart. This is another quick way to visualize day by day the behavior of a machine to see what has changed.

Figure 68. Traffic Profiles

11. Select Observations, then types, scroll down until you find Geographic Watchlist Observations, click the arrow next to it. As flows are processed each flow that matches a country on the watchlist will be listed here. This may be empty initially as the system is new, check in 24 hours to see how many flows are to high risk countries.

Figure 69. Wkst1 Observations



Summary

Within this lab you learned:

- The importance of accounting for all traffic to and from the Internet
- How to perform network retrospection to suspect countries
- How to detect research traffic for a host or external IP address.
- What alerts are linked with high risk countries.

☑ End of Lab: Please pause here.

Insider & Advanced Threat Detection

Lab 3: Data Exfiltration

Business Objective

One of the most valuable assets for an organization is its intellectual property, confidential information, and information stored in the company networks. Data breaches cost organizations millions of dollars.

Stealthwatch Cloud tracks inside and outside hosts to which an abnormal amount of data has been transferred. If a host triggers events exceeding a configured threshold, it results in an Exfiltration alarm. In this lab we do not have a baseline to compare to so we are going to simulate the traffic and check for observations that match that type of activity.

Optimally configure Stealthwatch Cloud to send alerts to a Cisco Teams room if you have access to create one.

Test Drive Objectives

Security events contribute index points to alarms. Alarms are grouped into Alarm categories.

The Suspect Data Loss security event is in the Exfiltration alarm category and based on observed flow rather than a number of default points assigned to the alarm category when the security event occurs.

When this event triggers, an inside host acting as a client has uploaded a cumulative amount of TCP or UDP payload data to an outside host, and the amount exceeds the threshold set in the policy applied to the inside host.

What does it mean when this alarms fires? A host is being used to upload more information to the Internet than is acceptable. This can be anything from someone using external backup services to maliciously exfiltrating corporate data.

Test Drive Requirements

- Stealthwatch Cloud Portal
- Any version of NetFlow from within the network
- Visibility of all host-to-host traffic from the core/distribution

Test Drive Outline

The “attacker” in this scenario will be sending a large file from the system to a host on the Internet. In the example given in this document we will use ncat, but you could also transfer a file to a web file storage system like Google Drive or Dropbox.

Ensure you are collecting full NetFlow somewhere along the path between the attacker and victim IP.

- In the following examples, the attacker IP address will be 198.19.20.36

A disgruntled employee has downloaded customer information from a database server and is now sending critical sensitive data to a destination outside of your network.

Transfer a large amount of data to your attacking system

The steps to conduct this attack will vary depending on the type of system that you are using both for your attack and for your file share.

If you are using Windows and copying the file across a Windows file share, use Windows Explorer to connect from the attacker system.

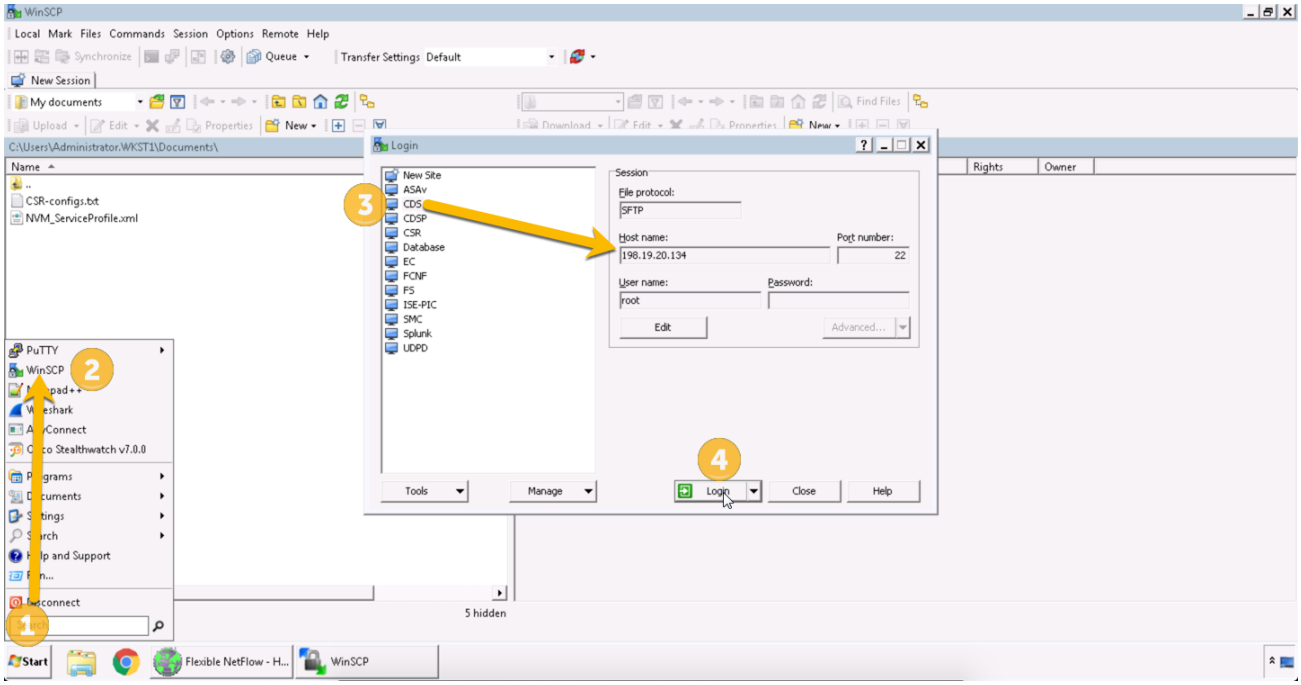
An FTP client would be used if you are connecting to a system serving files with an FTP server.

In this example, we will be transferring a 380 MB file via SCP from a database server to the Workstation 1within dCloud.

1. Select Start from Workstation 1, as shown below.
2. Select WinSCP, as shown below.
    a. Note: If an update appears, ignore the update.
3. Select CDS, as shown below.
    a. Note: The IP address of 198.19.20.134, the username and password are already cached for login.
4. Select Login and end C1sco12345 for the password.

    NOTE: If prompted with a certificate warning in WinSCP just click OK and continue.

Figure 70. Login WinSCP



5. Locate the file or files that you will be transferring. In this case it is the encrypted-customer-DB and transfer it to your downloads folder on the Workstation 1.
6. Initiate the transfer to the attacker system
7. Close WinSCP

Transfer a large amount of data from your attacking system

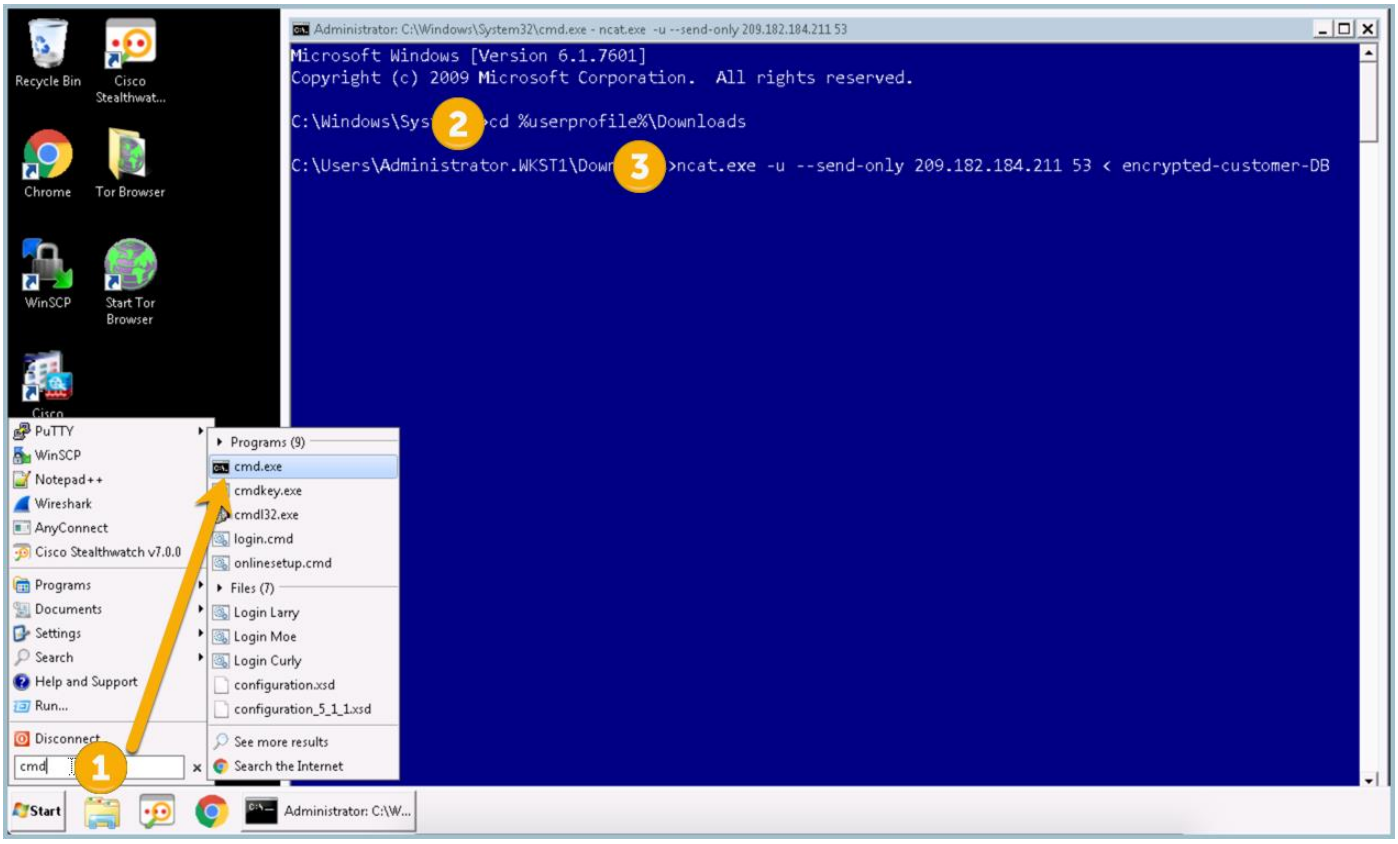
The steps to conduct this attack will vary depending on the type of system that you are using both for your attack and for your external file share.

An FTP client would be used if you are connecting to a system serving files with an FTP server, or you could use a web browser to transfer the file to a service such as Google Drive or Dropbox.

Transfer the 380 MB file to a remote host using ncat.

1. From Workstation 1, open cmd.exe to bring up the command prompt in Windows as illustrated below.
1. Change the directory to the Downloads directory using the change directory command: cd %userprofile%\Downloads in command prompt as shown below.
2. Enter %u the command prompt as illustrated below. Ncat.exe is used to stream the file to an external IP address. The –u option uses UDP as the protocol and 53 is the port.

Figure 71. ncat



Note: This could take up to several minutes to finish transferring. Be sure to check the Security Insight Dashboard for the Exfiltration alarm increasing.

While the tool is executing take a look at the following article:
https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?noredirect=on&utm_term=.e97851379584

Move on to the next lab, we will review the transfer activity later after it has been processed.

☑ End of Lab: Please pause here.

High Risk Application Detection

Lab 4: Detecting Internal Telnet Traffic

Business Objective

Many organizations prohibit the use of Telnet on the network. It is an unsecure protocol because it transfers data in clear text, introducing the risk of exposing login credentials to an attacker. Telnet can open an organization up to data loss. Mainframes and financial systems that contain customer information often run Telnet, leaving them vulnerable to network monitoring attacks.

Stealthwatch Custom Security Events can be created to alarm on unauthorized Telnet communications or other unwanted applications against a group of hosts.

Test Drive Objective

Security events contribute index points to alarms. Alarms are grouped into Alarm Categories.

The Policy Violations Alarm Category is a Custom Security event created to report on policy violations or unwanted communications in an organization.

Test Drive Requirements

The Stealthwatch system configuration minimum requirements are:

- Visibility of all host-to-host traffic from the core/distribution
- StealthWatch Cloud

Test Drive Outline

The “attacker” in this scenario will attempt to connect to a database using Telnet.

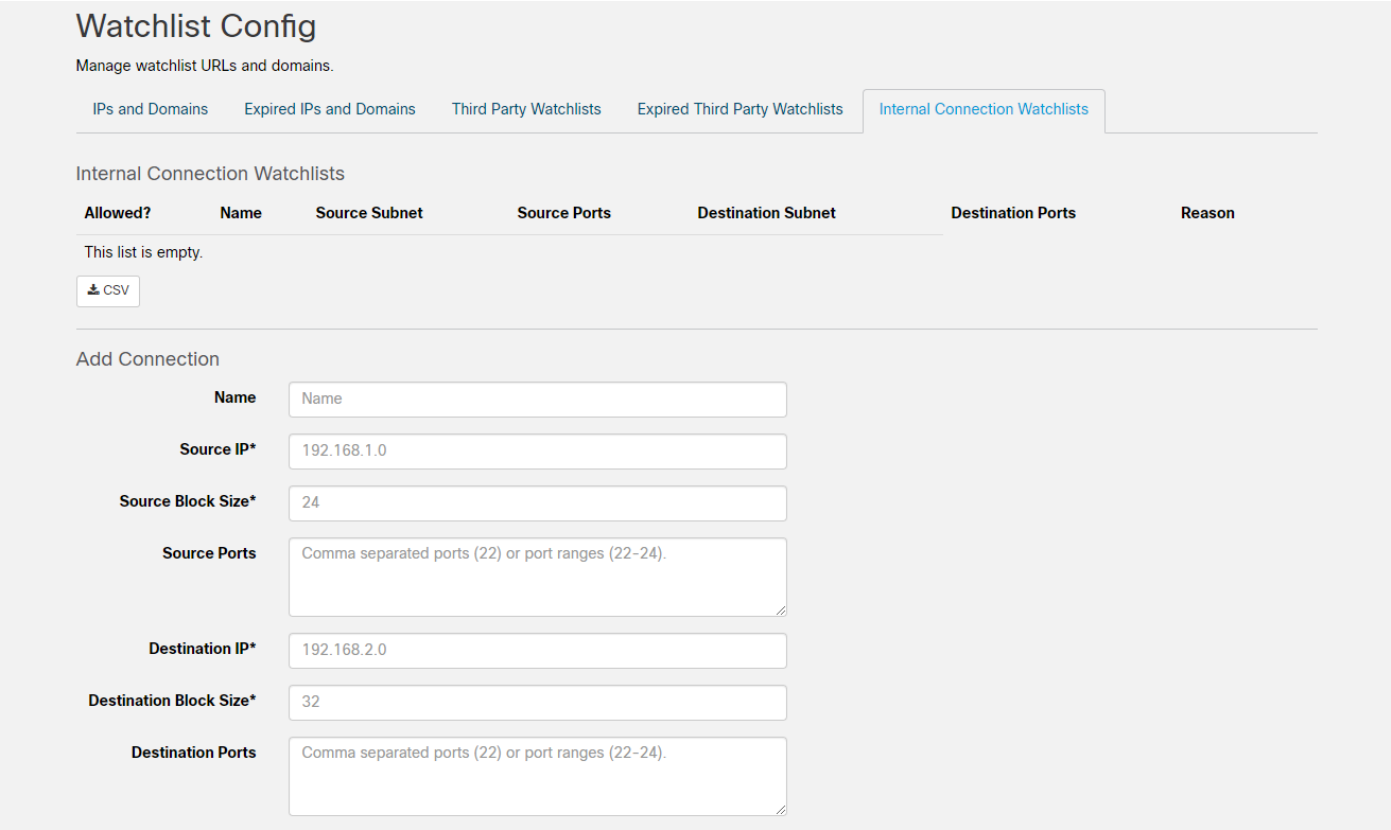
StealthWatch Cloud can use tripwires configured inside the network to catch unauthorized local and remote access. We will create a customer watchlists to detect this traffic.

Create an Internal Connect Watchlist to Detect Telnet Traffic Internally

In this lab, we set up a Custom watchlist to watch for telnet traffic to the 192.168.30.0/24 subnet, Telnet uses port 23/tcp. We could also create permit rules, these are similar to an ACL in that we can say some traffic is permitted, for example a legacy application that must use Telnet,

1. Open the Stealthwatch Cloud portal
2. Select Settings > Alerts, Configure Watchlists, Internal Connection Watchlist

Figure 72. Internal Connection Watchlist



Complete the following steps:

1. Enter Name: CSE: Telnet Traffic
2. Source IP: 198.19.30.0
3. Source Block Size: 24
4. Source Ports: 23
5. Destination Port IP: 0.0.0.0
6. Destination Block Size 0
7. Destination Ports: 0 - 65535
8. Reason: Telnet not permitted internally
9. Click Add

Figure 73. Watchlist Config

Enable the Telnet Server on Wkst1

In this task, we will enable the telnet server on the Wkst1 to show how easy it is for end users to expose risk to the organization.

Make sure the Telnet service is running:

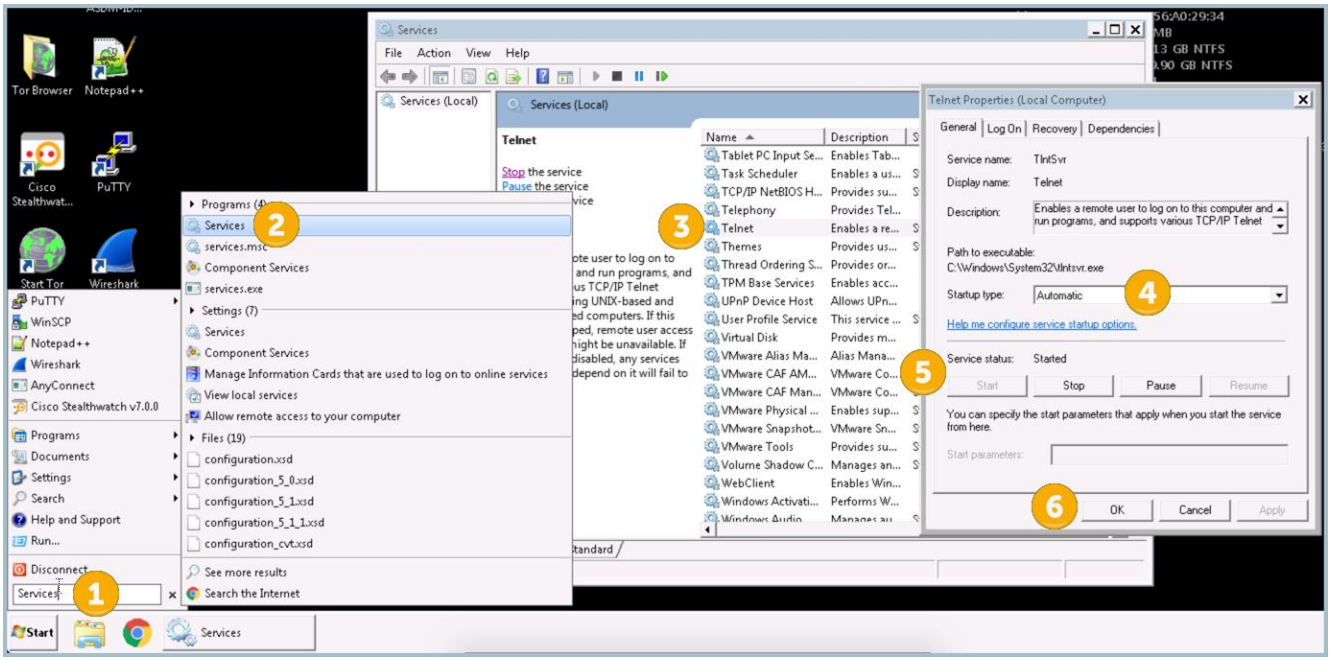
1. From the Remote Desktop Workstation select the Start button and search for Services
2. Open Services
3. Scroll down and double click on Telnet
4. Make sure the Startup Type is set to Automatic and select Apply
5. Select Start if the service is not running
6. Select Ok

Figure 74. Install Telnet

Make sure the Telnet service is running:

1. From the Remote Desktop Workstation select the Start button and search for Services
2. Open Services
3. Scroll down and double click on Telnet
4. Make sure the Startup Type is set to Automatic and select Apply
5. Select Start if the service is not running
6. Select Ok

Figure 75. Start Telnet



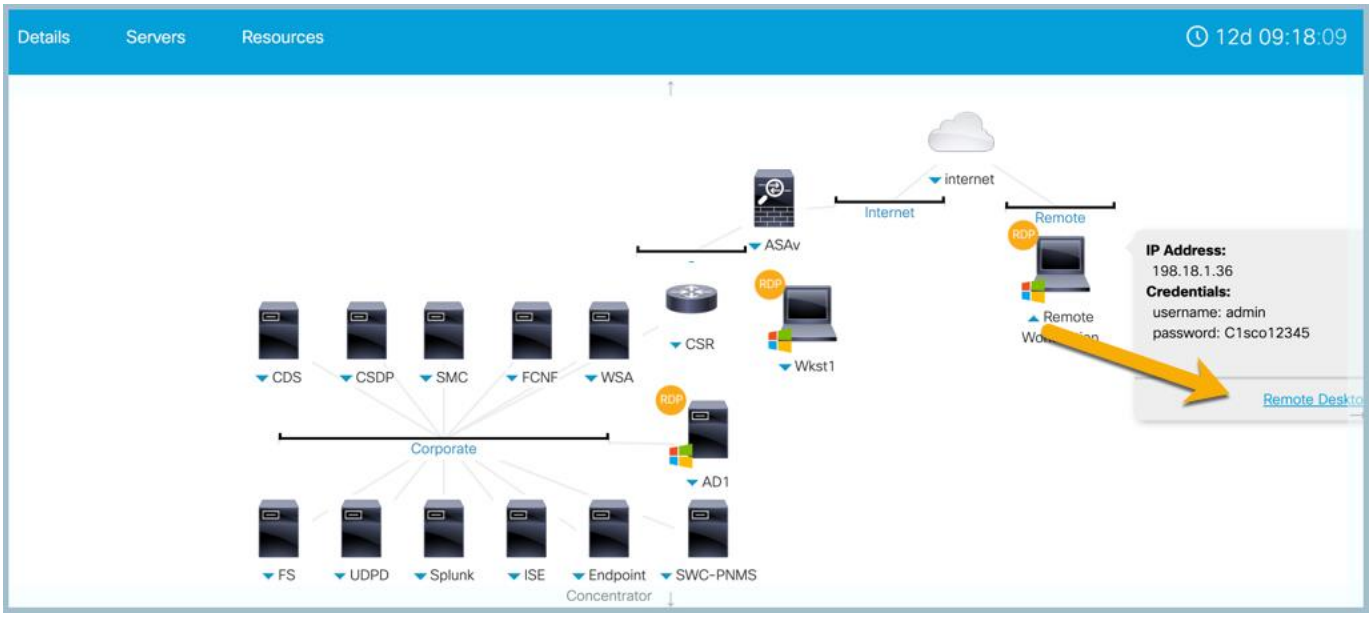
Connect to Server over Telnet from Remote VPN Workstation

In this task, we will use the Remote Workstation to connect to the Telnet server.

1. Open https://dcloud.cisco.com in a web browser and select My Hub
2. Select View for the current Cisco Stealthwatch 7.1 & ETA Test Drive Lab v2.2.
3. Select the Remote Desktop hyperlink under Remote Workstation as illustrated below.

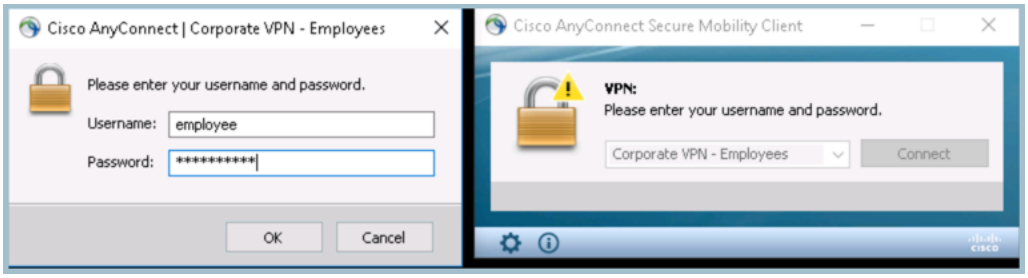
   NOTE: If you have trouble connecting to the Remote Desktop you may need to Reboot the workstation from the Servers utility.

Figure 76. Remote VPN



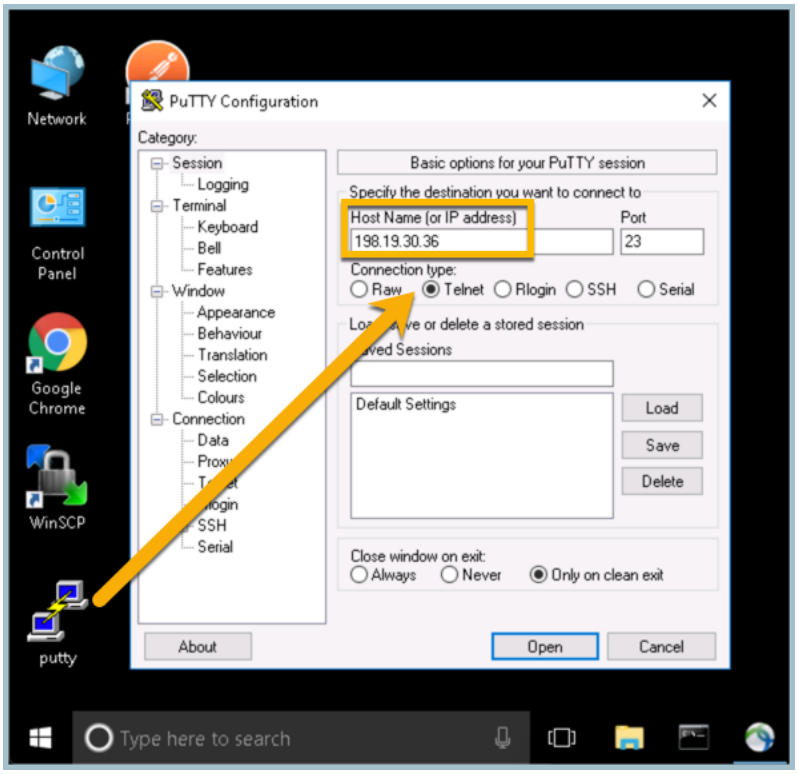
4. If prompted to login the username is admin and password C1sco12345.
5. Launch AnyConnect (if it does not automatically display; it is located in the services menu in the bottom right corner) and Login to Cisco AnyConnect Corporate VPN – Employees profile with username employee and password C1sco12345

Figure 77. AnyConnect



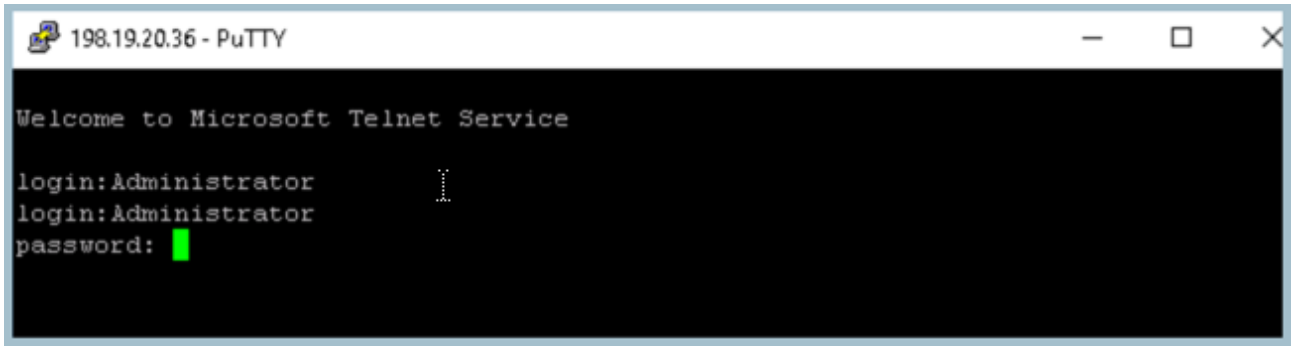
6. Launch Putty from the desktop and enter 198.19.30.36 in the host name field
7. Select Telnet

Figure 78. Putty



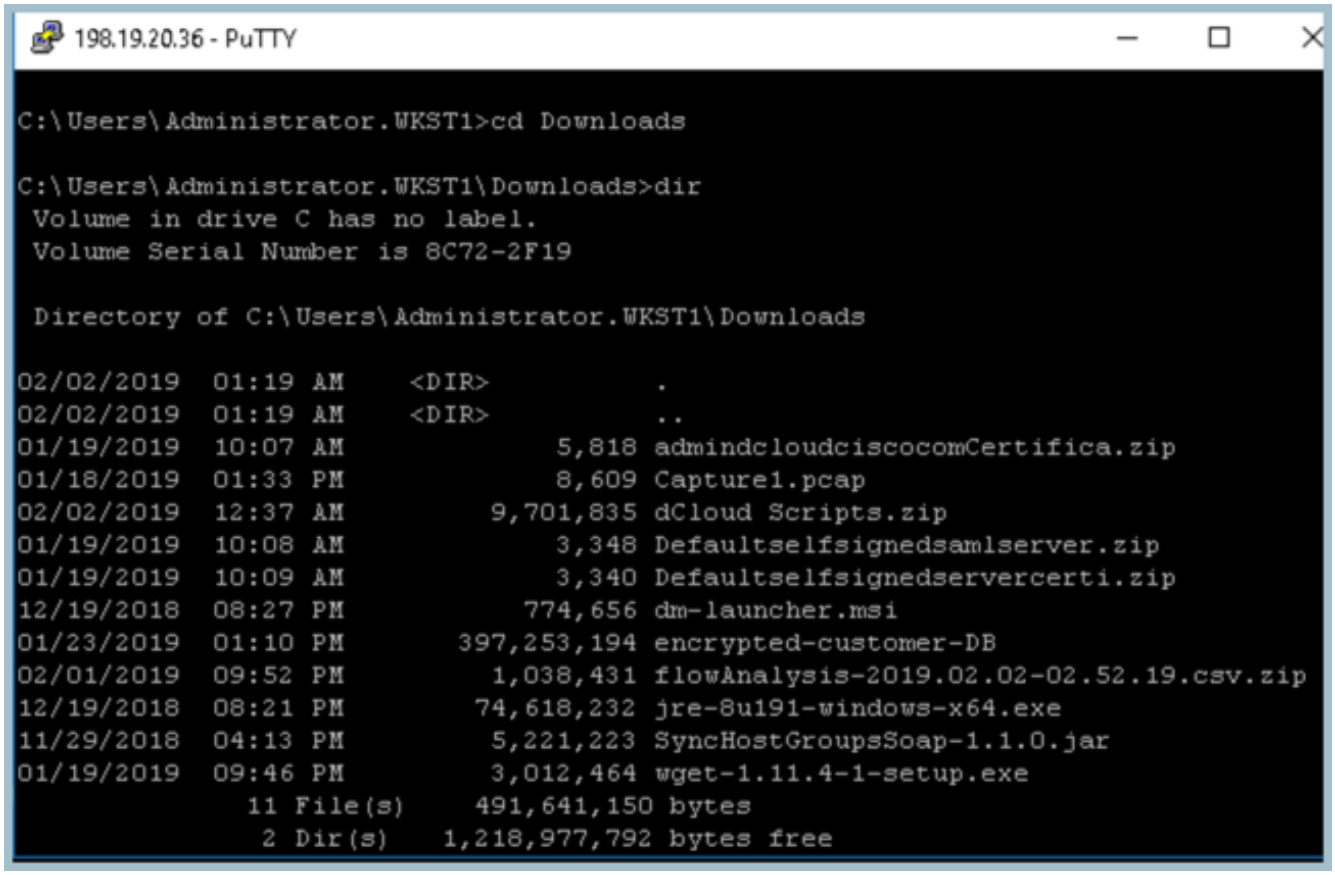
8. Press the Enter key to begin logging into the Telnet session use username Administrator with password C1sco12345 as illustrated below

Figure 79. Telnet



9. Run a few commands to validate you have a successful Telnet session into 198.19.30.36. Start with ipconfig to verify the IP address. Next enter cd Downloads and dir to list the directory as illustrated below. Type exit to drop the Telnet session and close the remote desktop session.

Figure 80. Talent Commands



It will take approx. 45 minutes for Stealthwatch Cloud to get the data and analyze it to produce the Internal Connection Watchlist hit alert. Check back on Alerts after you finish the ETA section.

StealthWatch Cloud includes a built-in assessment for risky traffic such as Telnet or unauthorized DNS. You will have access to the portal until the end of the week, to see the Visibility Assessment for your portal go to ? > Visibility Assessment. You can export a copy of the data in PDF for later reference.

Visibility Assessment Beta

PDF

Internal Monitored Network

Modern organizations need internal visibility to understand the state of their network and its traffic. Stealthwatch Cloud continuously monitors data transferred between servers and the Internet, and processes traffic flows. These metrics and others help security and network personnel quantify the hosts, systems, and resources on their network, making sure there is nothing present that they don't know about. It also helps identify critical assets, validate policies, audit and demonstrate compliance, and make better decisions based on data.

1,574	Hosts communicating within your network
3.1 TB	Internal traffic occurring on your network
134.2 GB	Traffic exchanged between your network and the internet
37.4 GB	Encrypted traffic exchanged between your network and the internet
27.9%	Fraction of encrypted traffic exchanged between your network and the internet
1	Active sensors
42,984,082	Flow records analyzed

External SMB Risk

Threat actors frequently target organizations by exploiting the Server Message Block (SMB) protocol to gain control of hosts. SMB is commonly used in many organizations and attackers use it to mask their activities on the network. Targeted destructive malware such as Conficker exploit vulnerabilities in SMB to deploy proxy tools, backdoors, and destructive tools. Stealthwatch Cloud monitors for hosts with many SMB sessions with hosts outside the network, which is consistent with worm propagation.

No External SMB traffic found in the past 30 days.

DNS Risk

DNS servers are critical to normal network function as they translate URLs to IP addresses. Many organizations utilize specific DNS servers to safeguard their network and enforce policies. When a host is found to be using an unauthorized DNS server, it could indicate malicious activity or policy violation. Malware may change a host's DNS server to forward request to sites used for phishing or exploit delivery. Likewise, network users may utilize unauthorized DNS servers to access web resources forbidden by internal policies.

Unauthorized DNS servers can:

Review Stealthwatch Observation for Unusual DNS activity

Earlier we transferred a large file using port 53 (DNS), Stealthwatch Cloud uses entity modeling and baselining to detect behavior deviations, since the portal we are using is new there is not enough of a baseline yet for some of the detections to generate. To see the flagged DNS activity, go to the Observations menu, the select By Types, scroll down to Unusual DNS Resolver and Unusual Packet Size Observations. Notice the DNS transfer we did earlier.

NOTE: you can connect back to the Remote VPN Workstation and use Nmap on the desktop to generate more traffic targeting the internal 198.19.20.0/24 subnet if you would like to explore more.

In this test case we created a custom security event to notify us if Stealthwatch ever sees internal Telnet traffic an alarm will fire as indicated above.

Telnet is an unsecure protocol with clear text traffic. It should never be used. This is just an example of how to create custom security events within Stealthwatch

Summary

Within this testing plan you learned:

- How to create a Custom Watchlist for Telnet communications
- How to simulate telnet traffic from the network
- How to access the Visibility Assessment
- Review the DNS Observation

Encrypted Traffic Analytics (ETA)

Business Objectives

The percentage of encrypted traffic over the public Internet has been increasing each year since the IP protocol began to support cryptography. The use of Internet Protocol (IP) Secure Sockets Layer (SSL) and Transport Layer Security (TLS) cryptography grew 90 percent from 2015 to 2016. Industry analysts from Gartner predict that more than 80 percent of all web traffic will be encrypted by 2019. Encrypted traffic hides possible threats to a network. Until recently, there was no way to analyze encrypted traffic without decrypting it; making it difficult to effectively monitor networks for threats. Cisco Encrypted Traffic Analytics addresses this problem by producing new telemetry data specifically derived from SSL / TLS connections. This data is then exported to a Stealthwatch Flow Collector where it is processed and stitched with connection data to provide new insights into network communications.

Using the Encrypted Traffic Analytics (ETA) technology, Stealthwatch detects malware in encrypted traffic without decryption by collecting network telemetry from Cisco IOS-XE devices including routers, switches, and Wireless LAN Controllers. Stealthwatch uses this data along with advanced entity modeling and multilayer machine learning to improve the fidelity of malware detection in encrypted traffic. These new techniques also use the Talos global threat map to identify and correlate known global threats to the local environment.

Requirements

Visit http://www.cisco.com/go/eta for an overview on ETA, how to enable it, and how to get started.

The Stealthwatch system configuration requirements are:

- Stealthwatch Cloud Portal
- ETA capable device
- Version 4 or newer of the Stealthwatch Cloud sensor

ETA capable platforms include the following devices (routers, switches or wireless LAN controllers running Cisco IOS-XE version 16.6 or later with a security feature license):

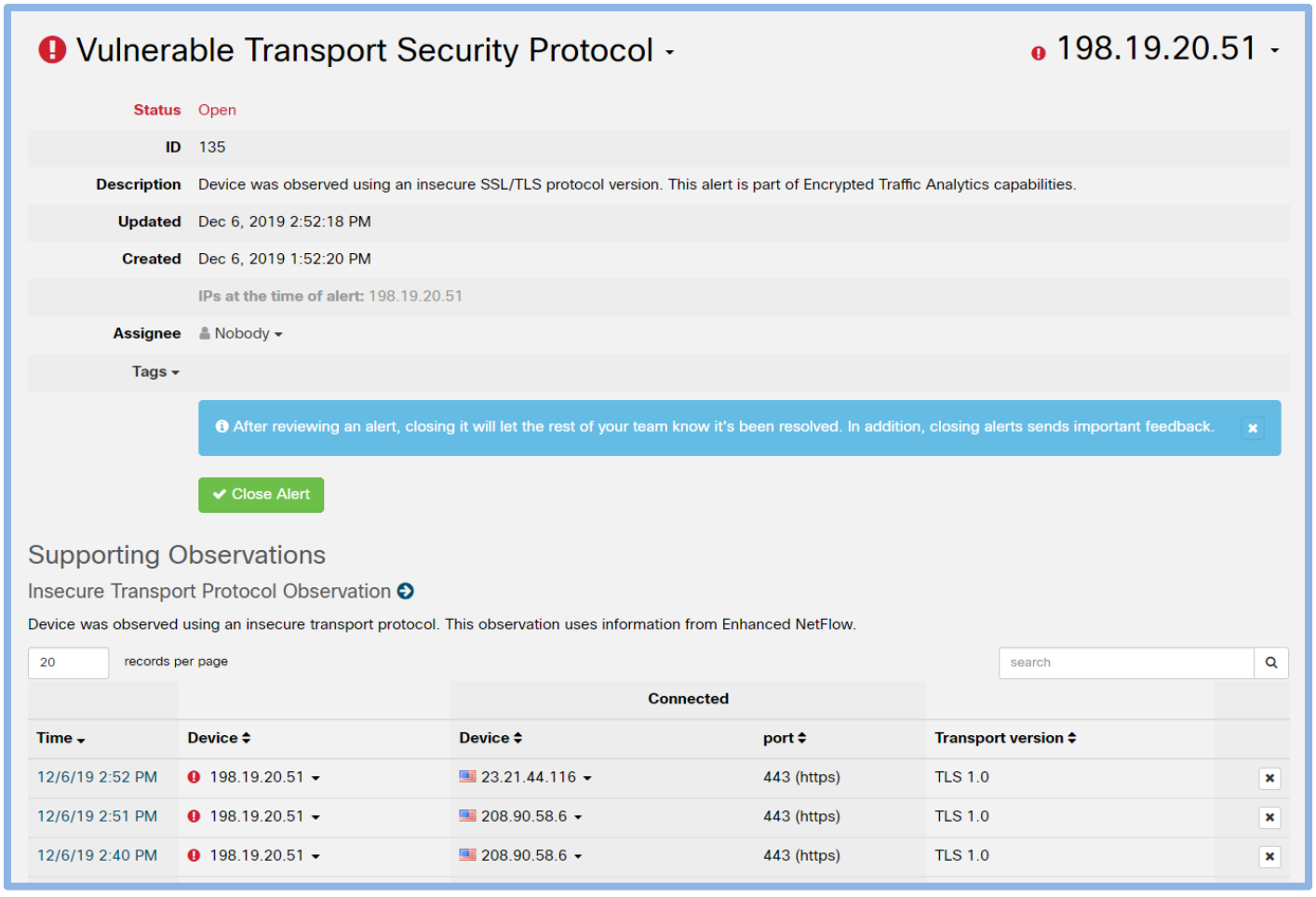
- Cisco Catalyst 9300 series switch
- ASR 1000 Series Aggregation Services Routers
- 4000 Series Integrated Services Routers
- Cloud Services Router 1000V Series
- Stealthwatch Flow Sensor v7.1 or later

Review Vulnerable Transport Alert

Stealthwatch cloud includes built-in alerts using Enhanced NetFlow + Cognitive (ETA) to perform additional detections.

1. Click on alerts in the main menu. There should be an auto generated alert for a machine using TLS1.0 which is important as browsers will soon stop supporting this version of TLS.
2. Select the Vulnerable Transport Protocol Alert which uses ETA for detection.

Figure 81. ETA Based Alert



Crypto audit to enforce authorized encryption standards

- Many organizations are interested in tools and techniques that can be used to better ensure the security of data and applications that they use. Using the ETA data and the Stealthwatch

Crypto Audit users can examine and report on cryptographic protocols and parameters used to establish encrypted communications to one or more hosts.

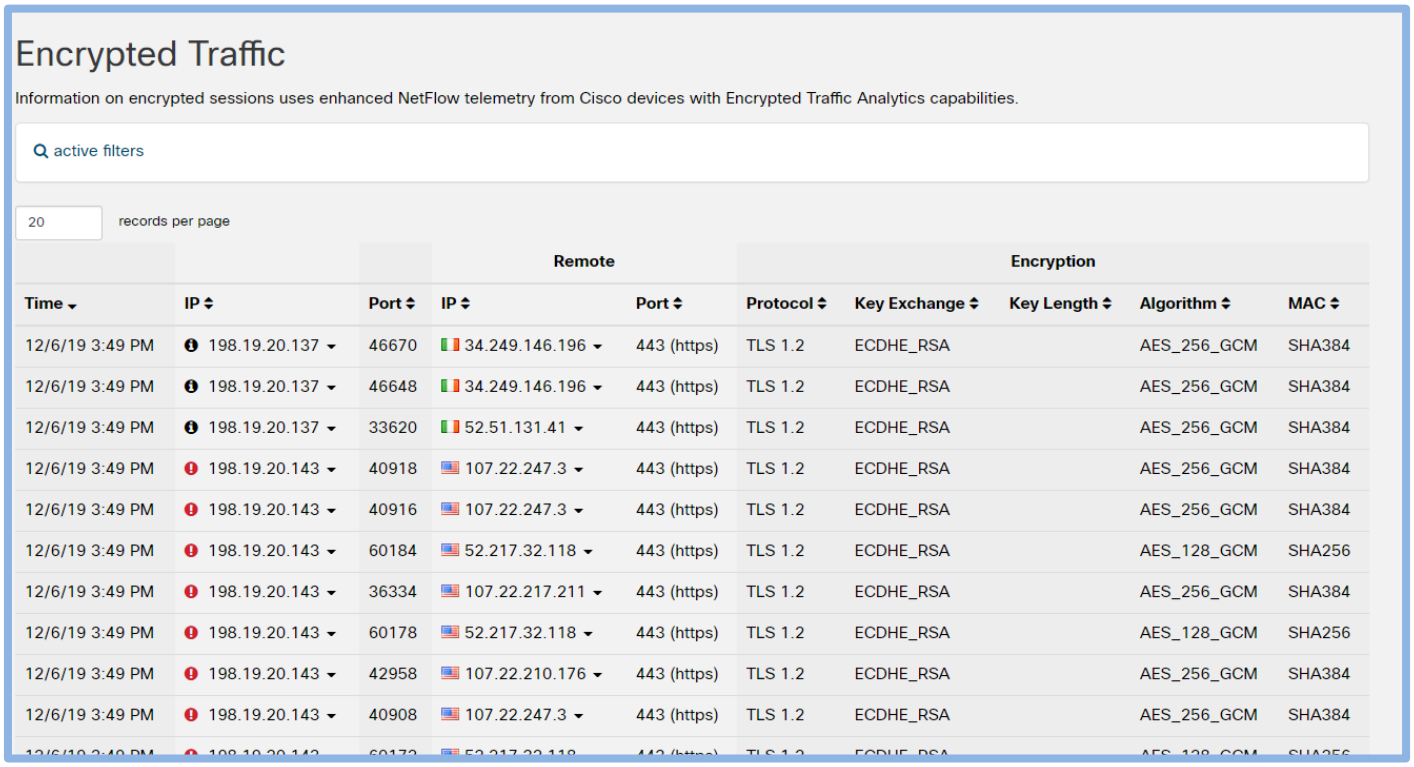
- Conduct and leverage a flow search to detect which encryption suites are being used on the network. Algorithms such as SHA-1 and RC4, as well as SSLv3 protocol are no longer considered secure. These algorithms and protocols are considered obsolete and are being retired by Microsoft and Google. They are being replaced by AES, RSA and SHA-3, and others.

Review Encrypted Traffic Query

Similar to the flow query we did earlier, Stealthwatch cloud includes a query to see what version of encryption are being used on the network.

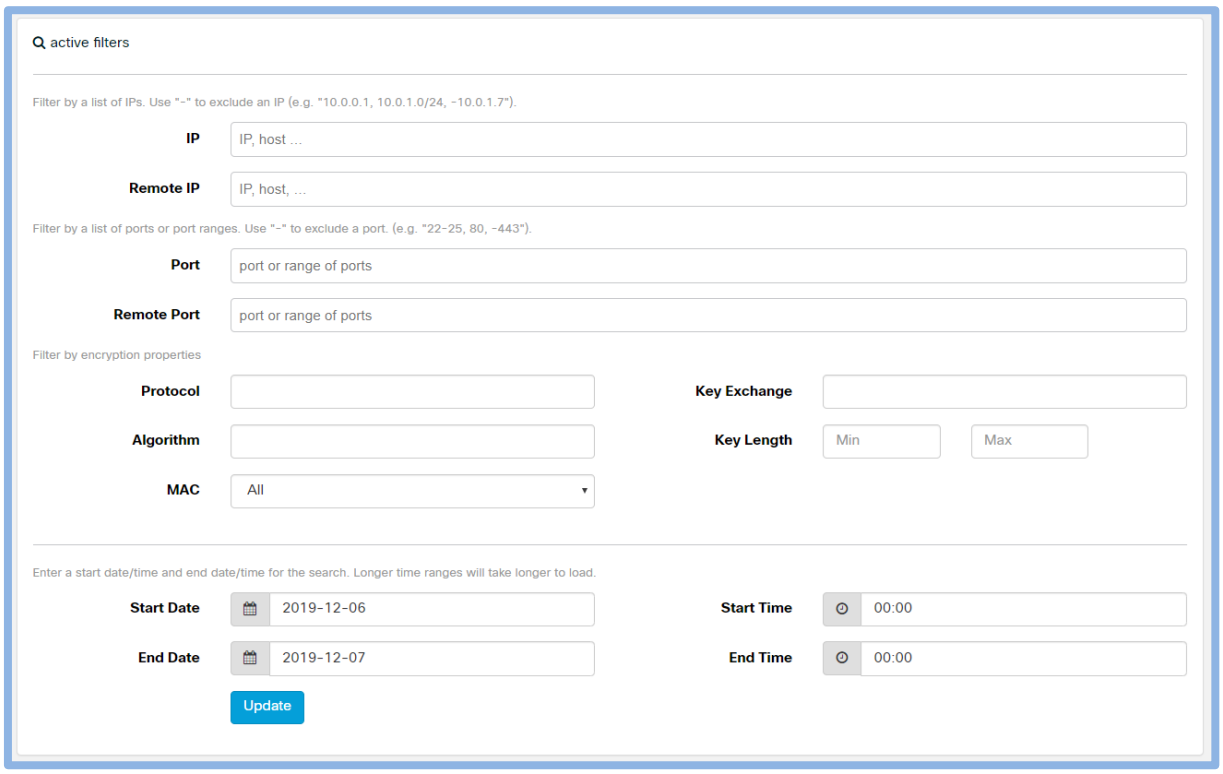
1. Click on Models in the main menu, then select Encrypted Traffic. Encryption data for the past 24 day will be displayed.

Figure 82. Encryption Query



2. Select Active Filters to expand the list of security filter options. Pick a few to see if they are present in this network. We already know TLS1.0 is being used, select TLS 1.3 in the protocol field to see what website are using that.

Figure 83. Encryption Filter Options



Appendix

Understanding NetFlow & IPFIX

Business Objectives

The primary data source of Stealthwatch is NetFlow. NetFlow is network traffic metadata that most current routers, switches and firewalls generate. This gives the administrator the ability to have 1-to-1 conversational visibility throughout a network. The conversations can be east-to-west client-to-client, or north-to-south client to Internet communications.

Test Drive Objectives

To fully understand Stealthwatch capabilities, you need a basic understanding of the different types of NetFlow, the devices that support NetFlow and the metadata that is contained in a NetFlow template. After this test drive, you will be able to articulate the different versions of NetFlow, types of supported NetFlow-capable devices and perform a basic Packet Capture (PCAP) analysis of NetFlow traffic.

Test Drive Requirements

The Stealthwatch system configuration minimum requirements are:

- NetFlow or IPFIX records that meet the minimum fields defined in this lab
- Visibility of all host-to-host traffic from the core, distribution, or access layer
- Any Stealthwatch version

Test Drive Outline

Someone from the NetOps team has called in and stated they have configured NetFlow on the router and switches in your infrastructure. You are looking at the Stealthwatch Management Console and don't see flows coming into the Flow Collector from the Security Insight Dashboard. You need to do some basic NetFlow troubleshooting by conducting a full packet capture on the Flow Collector and viewing the capture in Wireshark. You are provided NetFlow PCAPs in dCloud during this lab for analysis.

Lab: Understanding NetFlow

What is NetFlow?

NetFlow is a feature that was originally introduced on Cisco routers that provides the ability to collect IP network traffic as it enters or exits an interface. By analyzing the data provided by NetFlow, a network administrator can determine things such as the source and destination of traffic, class of service, and the causes of congestion.

What are the various kinds of NetFlow?

Most enterprise class networking devices today support some variant of NetFlow. These can go by different names, so you may run across one or more of these in client environments:

- FNF (Flexible NetFlow)
- NSEL (NetFlow Security Event Logging)
- IPFIX (IP Flow Information Export)
- TNF (Traditional NetFlow)

- FlowCache
- NetFlow-lite Phase 1
- NetFlow-lite Phase 2
- AVC (Application Visibility and Control)
- NBAR2 (Network-Based Application Recognition)
- sFlow (Sampled Flow)

These all differ in various ways, and some Cisco devices can export NBAR2 as part of AVC which can provide extra application information to assist in investigations with Stealthwatch.

What NetFlow information is Stealthwatch expecting to see?

Stealthwatch expects specific NetFlow fields to be passed for it to properly analyze network traffic. Together, these fields comprise the NetFlow template.

The most common issue experienced when setting up Stealthwatch is invalid template errors. On most devices, you will be able to modify the NetFlow fields sent to Stealthwatch to receive the proper template information. For those devices that cannot send the proper template information, you will need to either rely on the NetFlow generated by other devices or install a device like a Stealthwatch Flow Sensor to generate NetFlow that Stealthwatch can interpret for you.

The Required and Optional NetFlow fields that Stealthwatch ingests are:

Description	*Required or Optional?*	*Notes*
match ipv4 protocol	Required	Key field
match ipv4 source address	Required	Key field
match ipv4 destination address	Required	Key field
match transport source-port	Required	Key field
match transport destination-port	Required	Key field
match interface input	Required	Key field
match ipv4 tos	Required	Key field
collect interface output	Required	Key field

collect counter bytes	Required	Key field
collect counter packets	Required	Key field
collect timestamp sys-uptime first	Required	For calculating duration
collect timestamp sys-uptime last	Required	For calculating duration
collect routing next-hop address ipv4	Optional	Used for closest interface determination
collect ipv4 dscp	Optional	Used for closest QoS monitoring
collect ipv4 ttl minimum	Optional	Used for to understand the path of flow
collect ipv4 ttl maximum	Optional	Used for to understand the path of flow
collect transport tcp flags	Optional	Used for reporting on TCP flags
collect routing destination AS	Optional	Used for AS reporting
collect application name	Optional	Used to capture layer 7 application name when NBAR2 is being used
collect application http host	Optional	Used to capture URL information when AVC is being used

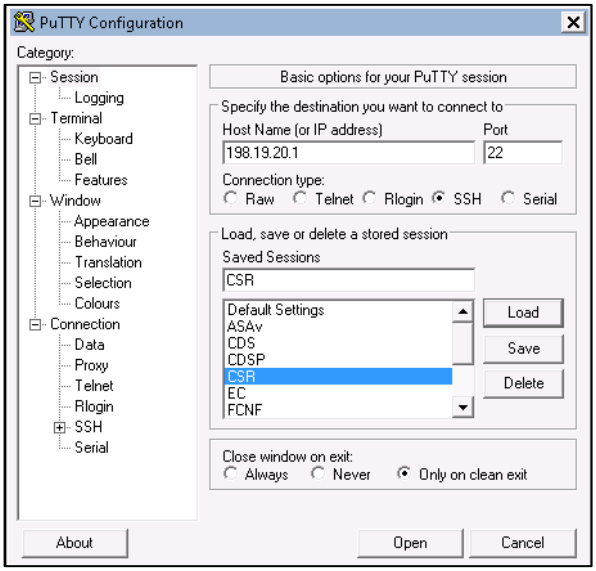
Steps to enable flow

1. Create a Flow Record
2. Configure the Exporter
3. Configure the Monitor
4. Configure the Interface(s)

View flow configurations from the CSR Router

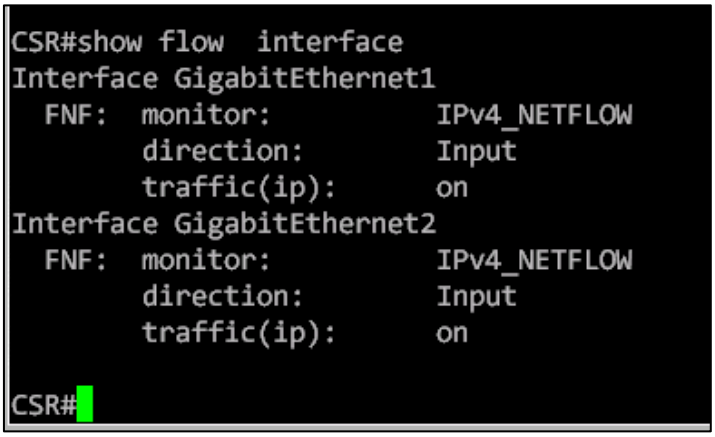
1. Open Putty, load the CSR configuration and open the session as shown below:

Figure 84. Putty Configuration



2. The session will load with the username admin
    a. Insert the password of C1sco12345
3. Use the following command to view the interfaces flow is being exported from
    a. show flow interface
4. You should the output as shown:

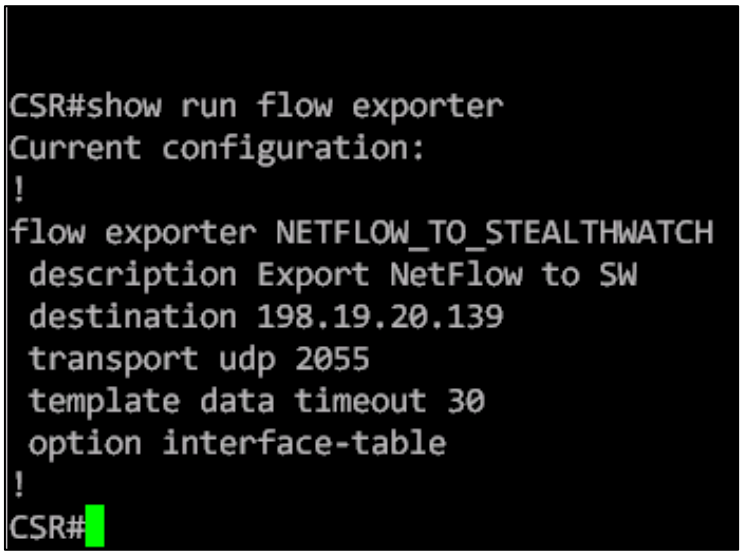
Figure 85. Show flow interface



Note: The direction of the flow: Input. When enabling flow, it is best practice to enable flow on the interface in the ingress direction

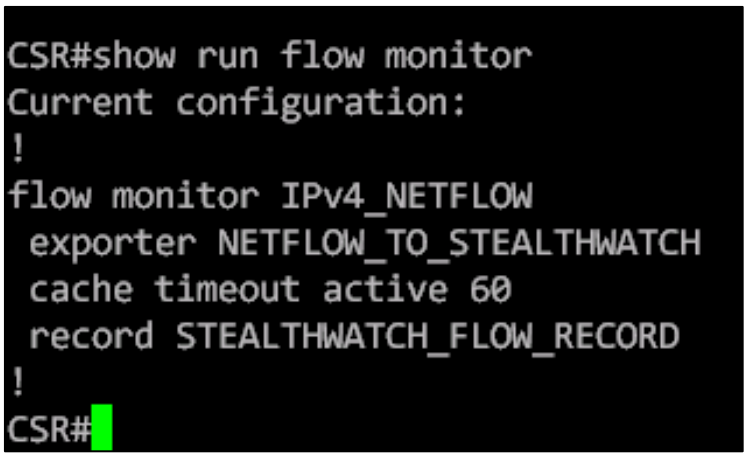
5. View the flow exporter with the following command:
    a. show run flow exporter
6. The output should be the same as below

Figure 86. Show flow exporter



7. Issue the following command:
    a. show run flow monitor
8. The output should be the same as below:

Figure 87. Show flow monitor



Note: The cache timeout on Cisco devices be default is 30 minutes. Stealthwatch needs the cache active timeout to be 1 minute or 60 seconds.

9. Issue the command
    a. show run flow record
10. Take note of the output shown below:

Figure 88. Show flow record

```
CSR#show run flow record
Current configuration:
!
flow record STEALTHWATCH_FLOW_RECORD
 description NetFlow record for SW
 match ipv4 tos
 match ipv4 source address
 match ipv4 destination address
 match transport destination-port
 match transport source-port
 match interface input
 match ipv4 protocol
 collect routing source as
 collect routing destination as
 collect routing next-hop address ipv4
 collect ipv4 dscp
 collect ipv4 id
 collect ipv4 source prefix
 collect ipv4 source mask
 collect ipv4 destination mask
 collect ipv4 ttl minimum
 collect ipv4 ttl maximum
 collect transport tcp flags
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
CSR#
```

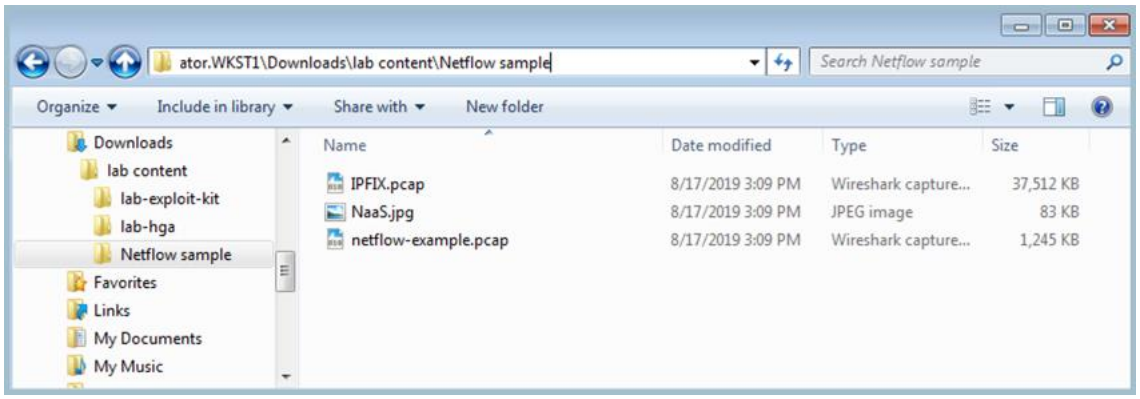
Note: The highlighted match and collect statements above are required fields in Stealthwatch. The other fields are optional to collect additional data.

Review this tool that was built by a Cisco engineering on sample NetFlow configurations on a per devices bases: https://configurenetflow.info/. This is a good resourced when having NetFlow enabled within your environment.

Reviewing a NetFlow Packet Capture

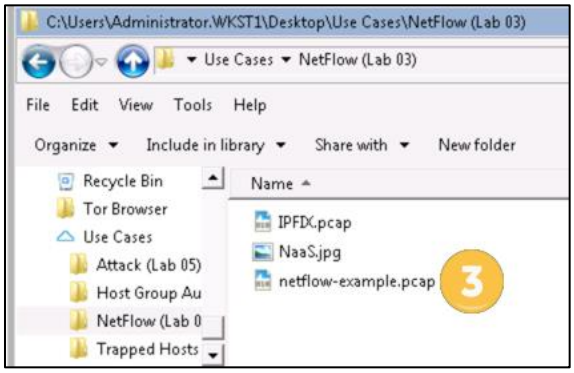
1. From Wkst1, open the Downloads > lab content from Windows Explorer.
2. Open the NetFlow sample folder

Figure 89. NetFlow sample pcaps



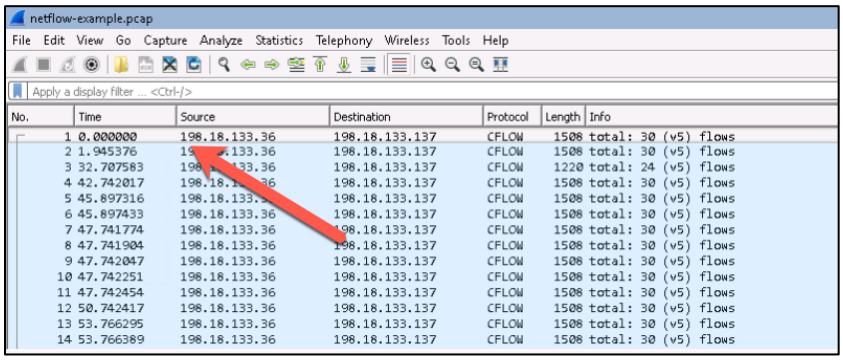
3. Open the netflow-example.pcap file
    a. Note: If a Wireshark update window appears, select skip this version.

Figure 90. NetFlow-example.pcap file



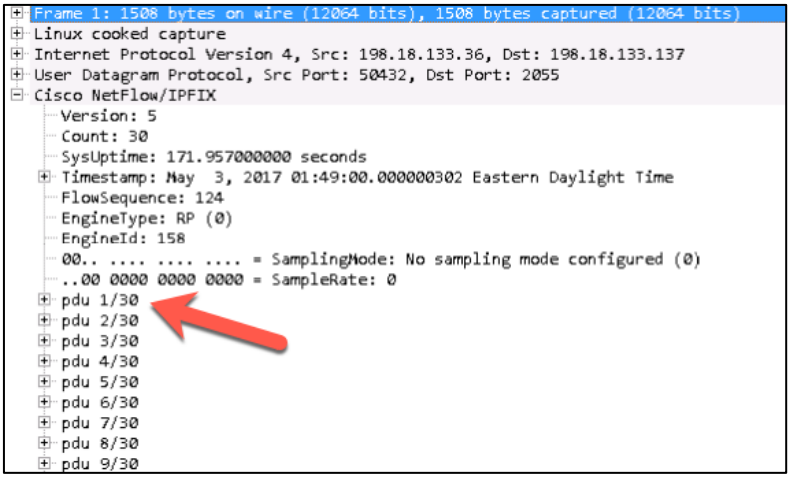
4. Select the first packet from the capture

Figure 91. Wireshark packet listing of **netflow-example.pcap**



5. In the middle section of Wireshark, click the + next to Cisco NetFlow/IPFIX

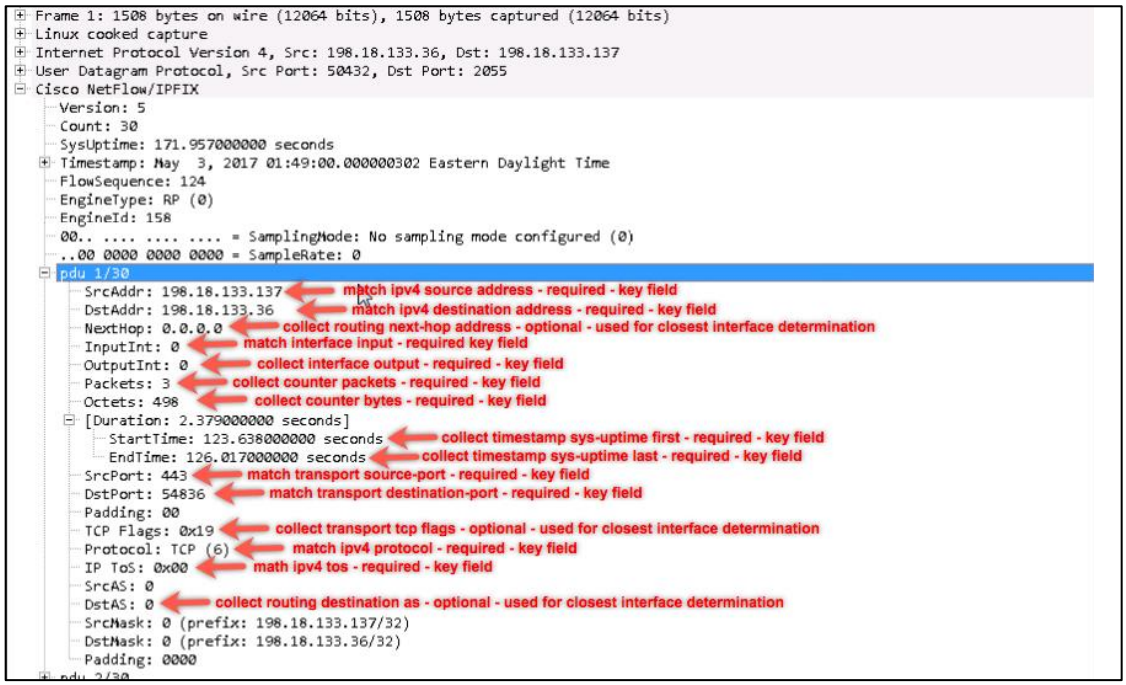
Figure 92. Packet details of netflow-example.pcap



Click to expand one of the PDU's as shown above. PDU is short for Protocol Data Unit. The term used to describe data as it moves from one layer of the OSI model to another. In this reference, PDU is often used synonymously with packet.

6. Compare the fields in the pdu to the figure below.

Figure 93. Expanded PDU



You may need to do a similar analysis of a packet if Stealthwatch is giving invalid template errors for a device, and the configuration looks accurate.

If any NetFlow fields are missing, like the source IP, time stamps, or byte counters that Stealthwatch requires, you will need to have the NetFlow record on the source exporters adjusted to contain the minimum required fields.

Summary

In this lab you learned:

- That Stealthwatch uses NetFlow as its primary data source
- The different types of NetFlow
- Which NetFlow fields are required versus optional
- How to decode a NetFlow packet with Wireshark
- How to decode an IPFIX packet with Wireshark

☑ End of Lab: Please pause here.